PX-1000 Series

User Guide

Release 2.1.5

DPX2-1000-0B-v2.1.5-E

March 2011

255-80-6105-00

Safety Guidelines

WARNING! Read and understand all sections in this guide before installing or operating this product.

WARNING! Connect this product to an AC power source whose voltage is within the range specified on the product's nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to an AC power source that is current limited by a suitably rated fuse or circuit breaker in accordance with national and local electrical codes. Operating this product without proper current limiting may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a protective earth ground. Never use a "ground lift adaptor" between the product's plug and the wall receptacle. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury and death.

WARNING! This product contains no user serviceable parts. Do not open, alter or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury and death.

WARNING! Use this product in a dry location. Failure to use this product in a dry location may result in electric shock, personal injury and death.

WARNING! Do not rely on this product's receptacle lamps, receptacle relay switches or any other receptacle power on/off indicator to determine whether power is being supplied to a receptacle. Unplug a device connected to this product before performing repair, maintenance or service on the device. Failure to unplug a device before servicing it may result in electric shock, fire, personal injury and death.

WARNING! Only use this product to power information technology equipment that has a UL/IEC 60950-1 or equivalent rating. Attempting to power non-rated devices may result in electric shock, fire, personal injury and death.

WARNING! Do not use this product to power inductive loads such as motors or compressors. Attempting to power inductive loads may result in damage to the product.

WARNING! Do not use this product to power critical patient care equipment, fire or smoke alarm systems. Use of this product to power such equipment may result in personal injury and death.

WARNING! If this product is a model that requires assembly of its line cord or plug, all such assembly must be performed by a licensed electrician and the line cord or plugs used must be suitably rated based on the product's nameplate ratings and national and local electrical codes. Assembly by unlicensed electricians or failure to use suitably rated line cords or plugs may result in electric shock, fire, personal injury or death.

WARNING! This product contains a chemical known to the State of California to cause cancer, birth defects, or other reproductive harm.

Safety Instructions

1. Installation of this product should only be performed by a person who has knowledge and experience with electric power.
2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.
3. This product is designed to be used within an electronic equipment rack. The metal case of this product is electrically bonded to the line cord ground wire. A threaded grounding point on the case may be used as an additional means of protectively grounding this product and the rack.
4. Examine the branch circuit receptacle that will supply electric power to this product. Make sure the receptacle’s power lines, neutral and protective earth ground pins are wired correctly and are the correct voltage and phase. Make sure the branch circuit receptacle is protected by a suitably rated fuse or circuit breaker.
5. If the product is a model that contains receptacles that can be switched on/off, electric power may still be present at a receptacle even when it is switched off.

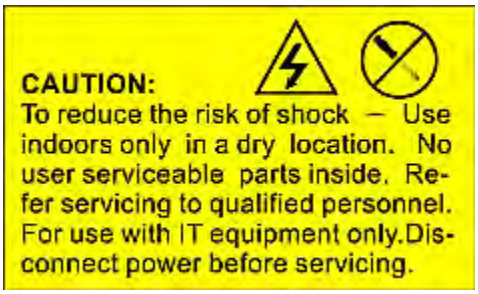
FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.



Contents

Applicable Models

This user guide is applicable to the **PX-1000 series**, whose model name follows the **PX2-1nnn** format, where n is a number.

Note: For information on PX2-3nnn, PX2-4nnn and PX2-5nnn series, see the "PX2-3000/4000/5000 Series" User Guide or online help.

What's New in the Dominion PX User Guide

The following sections have changed or information has been added to the Dominion PX User Guide based on enhancements and changes to the equipment and/or user documentation.

Please see the Release Notes for a more detailed explanation of the changes applied to this version of Dominion PX.

Chapter 1 Introduction

Dominion PX is an intelligent power distribution unit (PDU). The intended use of the Raritan Dominion PX is distribution of power to information technology equipment such as computers and communication equipment where such equipment is typically mounted in an equipment rack located in an information technology equipment room.

With Dominion PX, you can remotely monitor power to devices in the data center and keep track or be notified of any significant power events or alerts.

In This Chapter

Product Models

Dominion PX comes in several models that are built to stock and can be obtained almost immediately. Raritan also offers custom models that are built to order and can only be obtained on request.

Visit the ***Product Selector page*** (***http://www.raritan.com/resources/px-product-selector/***) on the Raritan website or contact your local reseller for a list of available models.

Product Features

Dominion PX models vary in sizes and features. In general, Dominion PX features include:

- The ability to monitor the following at the inlet level:
  - Active energy (Wh)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - RMS current per line (A)
  - RMS voltage per line pair (V)
- The ability to monitor the following at the circuit breaker level:
  - Status (closed/open)
  - Current drawn (A)
  - Current remaining (A)

- The ability to monitor environmental factors such as external temperature and humidity
- User-specified location attributes for environmental sensors
- An audible alarm (beeper) to indicate current overload
- Configurable alarm thresholds and hysteresis
- Configurable assertion timeout for thresholds
- The ability to remotely track the locations of IT devices on the rack through connected asset sensors
- Support for SNMP v1, v2, and v3
- The ability to send traps using the SNMP protocol
- The ability to store a data log of all sensor measurements and retrieve it via SNMP

  Note: Raritan's Power IQ or other external systems can retrieve the stored data (samples) from Dominion PX.

- The ability to configure and set values through SNMP, including power threshold levels
- The ability to save one Dominion PX device's configuration settings and then deploy those settings to other Dominion PX devices
- Local overcurrent protection (OCP) via branch circuit breakers or fuses on products rated over 20A to protect connected equipment against overload and short circuits
- Measurement accuracy for the inlet:

  Voltage: 1%

  Current: 1%+/-0.1A

  Active power: 1%

  Active energy: 1%

- A combination of outlet types (for example, C13 and C19 outlets) in select models
- A combination of outlet voltages (120 and 208 volts) in select models
- Support for high current devices (such as Blade Servers) in select models
- The ability to diagnose the network, such as pinging a host or listing TCP connections
- Full disaster recovery option in case of a catastrophic failure during a firmware upgrade

Package Contents

The following sub-topics describe the equipment and other material included in the product package.

Zero U Products

- Dominion PX device
- Screws, brackets and/or buttons for Zero U
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for outlets or the inlet (for PX-1000 series only)

1U Products

- Dominion PX device
- 1U bracket pack and screws
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for outlets or the inlet (for PX-1000 series only)

2U Products

- Dominion PX device
- 2U bracket pack and screws
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for outlets or the inlet (for PX-1000 series only)

Chapter 2 Rack-Mounting the PDU

This chapter describes how to rackmount a Zero U Dominion PX device. To mount a PX-1000 series PDU, you can use either two buttons or L-brackets that Raritan provided.

In This Chapter

Rackmount Safety Guidelines

In Raritan products which require rack mounting, follow these precautions:

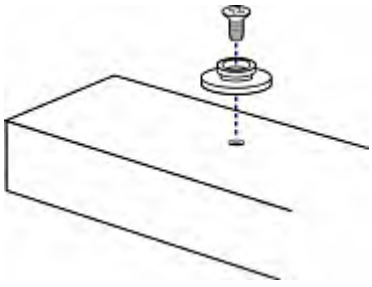
- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the Power Distribution Units. See ***Specifications*** (on page 222) in the User Guide.
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, to the branch circuit.

Mounting Zero U Models Using Two Rear Buttons

The following describes how to mount a PDU using two buttons only.

To mount Zero U models using two buttons:

1. Turn to the rear of the PDU.
2. Locate two screw holes on the rear panel: one near the bottom and the other near the top (the side of cable gland).
3. Screw a button in the screw hole near the bottom. The recommended torque for the button is 1.96 N·m (20 kgf·cm).

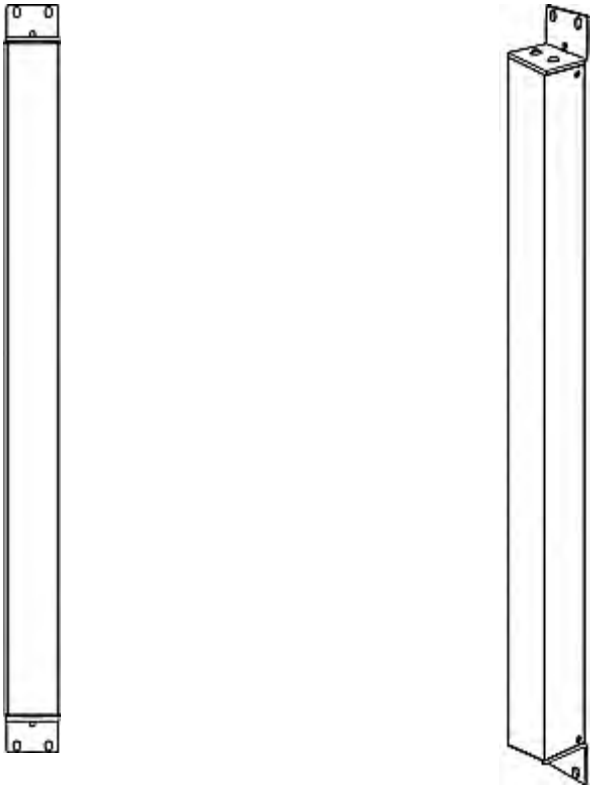


4. Screw a button in the screw hole near the top. The recommended torque for the button is 1.96 N·m (20 kgf·cm).

5. Ensure that the two buttons can engage their mounting holes in the rack or cabinet simultaneously.
6. Press the Dominion PX device forward, pushing the mounting buttons through the mounting holes, then letting the device drop slightly. This secures the Dominion PX device in place and completes the installation.

Mounting Zero U Models Using L-Brackets and Buttons

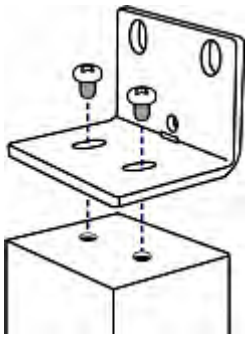
This section describes how to mount a PX-1000 series PDU using L-brackets and two buttons.



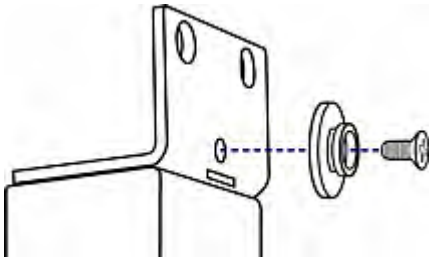
To mount Zero U models using L-brackets and two buttons:

1. Align the two central holes of the L-bracket with the two screw holes on the top of the PDU.

2. Screw the L-bracket to the PDU and ensure the bracket is fastened securely.



3. Repeat Steps 1 to 2 to screw another L-bracket to the bottom of the PDU.
4. After both L-brackets are installed on the PDU, you can choose either of the following ways to mount the PDU in the rack.
   - Using rack screws, fasten the PDU to the rack through the two upper holes of each L-bracket.
   - Mount the PDU by screwing a mounting button in the back center of each L-bracket and then having both buttons engage the mounting holes in the rack. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



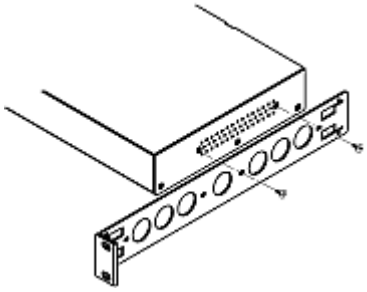
Mounting 1U or 2U Models

Using the appropriate brackets and tools, fasten the 1U Dominion PX device to the rack or cabinet.

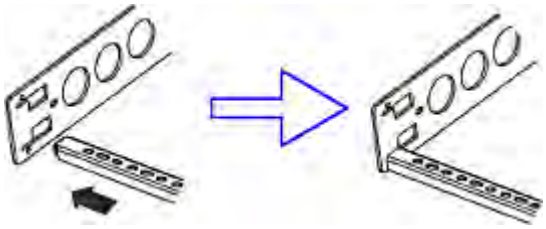
To mount the Dominion PX device:

1. Attach one rackmount bracket to one side of the Dominion PX device.
   a. Align two oval-shaped holes of the rackmount bracket with two threaded holes on one side of the Dominion PX device.
   b. Secure the rackmount bracket with two of the Raritan-provided screws.

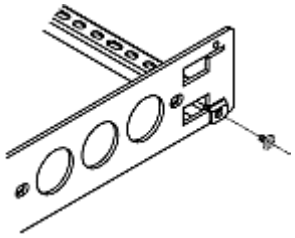
Note: The appropriate oval-shaped hole locations of the rackmount bracket may vary according to the threaded holes on you model.



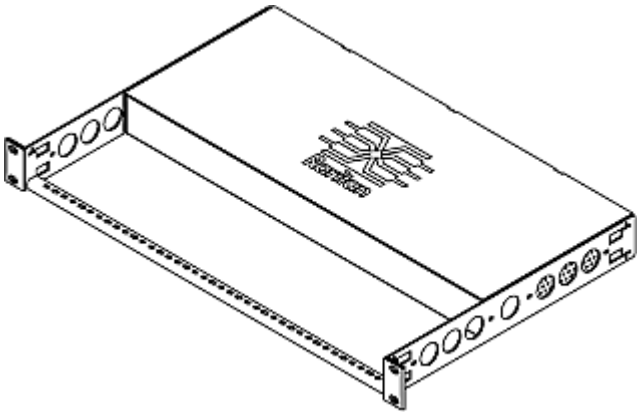
2. Repeat Step 1 for securing the other rackmount bracket to the other side of Dominion PX.
3. Insert one end of the cable-support bar into the L-shaped hole of the rackmount bracket, and align the hole on the end of the bar with the threaded hole adjacent to the L-shaped hole.



4. Secure the cable-support bar with one of the Raritan-provided cap screws.



5. Repeat Steps 3 to 4 to secure the other end of the cable-support bar to the other rackmount bracket.



Mount the Dominion PX device on the rack by securing the rackmount brackets' ears to the rack's front rails with your own screws, bolts, cage nuts, or the like.

Chapter 3 Installation and Configuration

This chapter explains how to install a Dominion PX device and configure it for network connectivity.

In This Chapter

Before You Begin

Before beginning the installation, perform the following activities:

- Unpack the product and components
- Prepare the installation site
- Fill out the equipment setup worksheet

Unpacking the Product and Components

1. Remove the Dominion PX device and other equipment from the box in which they were shipped. See ***Package Contents*** (on page 2) for a complete list of the contents of the box.
2. Compare the serial number of the equipment with the number on the packing slip located on the outside of the box and make sure they match.
3. Inspect the equipment carefully. If any of the equipment is damaged or missing, contact Raritan's Technical Support Department for assistance.
4. Verify that all circuit breakers on the Dominion PX device are set to ON. If not, turn them ON.

   For a PDU with fuses, ensure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

   Note: Not all Dominion PX devices have overcurrent protection mechanisms.

Preparing the Installation Site

1. Make sure the installation area is clean and free of extreme temperatures and humidity.

Note: If necessary, contact Raritan Technical Support for the maximum operating temperature for your model. See **Maximum Ambient Operating Temperature** *(on page 222).*

2. Allow sufficient space around the Dominion PX device for cabling and outlet connections.
3. Review the ***Safety Instructions*** (on page iii) listed in the beginning of this user guide.

Filling Out the Equipment Setup Worksheet

An Equipment Setup Worksheet is provided in this guide. See ***Equipment Setup Worksheet*** (on page 224). Use this worksheet to record the model, serial number, and use of each IT device connected to Dominion PX.

As you add and remove devices, keep the worksheet up-to-date.

Checking the Branch Circuit Rating

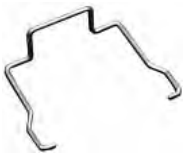
This section describes the rating of the branch circuit supplying power to the PDU:

- The rating of the branch circuit shall be in accordance with national and local electrical codes.
- For North American, the rating of the branch circuit may be up to 125% greater than the rating of the PDU, unless prohibited by national or local electrical codes.
  - 20A for PDUs rated at 16A input current
  - 30A for PDUs rated at 24A input current
  - 40A for PDUs rated at 32A input current
  - 50A for PDUs rated at 35A input current
  - 50A for PDUs rated at 40A input current
  - 60A for PDUs rated at 45A input current
- In North America, external overcurrent protectors shall be certified by UL/CSA (or equivalent certification). In other regions or countries, make sure they comply with national and local electrical codes.

Installing Cable Retention Clips (Optional)

If your Dominion PX device is designed to use a cable retention clip, install the clip before connecting a power cord. A cable retention clip prevents the connected power cord from coming loose or falling off.

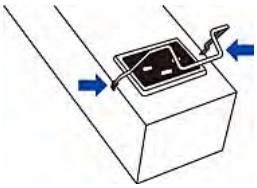
These optional clips come in various sizes to accommodate diverse power cords used on IT equipment, which are connected to C13 or C19 outlets. You can request a cable retention kit containing different sizes of clips from you reseller. Make sure you use a clip that fits the power cord snugly to facilitate the installation or removal operation (for servicing).



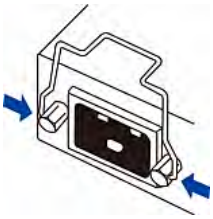
To install and use a cable retention clip:

1. Locate two tiny holes adjacent to the outlet (or inlet).
2. Install the cable retention clip by inserting two ends of the clip into the tiny holes.

Zero U models

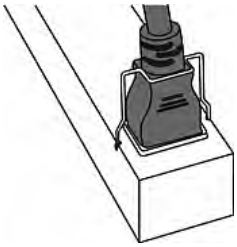


1U models

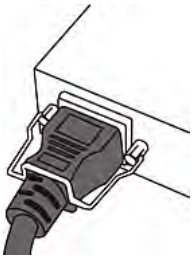


3. Connect the power cord to the outlet (or inlet), and press the clip toward the power cord until it holds the cord firmly.

Zero U models



1U models



Connecting the PDU to a Power Source

1. Verify that all circuit breakers on the Dominion PX device are set to ON. If not, turn them ON.

   For a PDU with fuses, ensure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

   Note: Not all Dominion PX devices have overcurrent protection mechanisms.

2. Connect each Dominion PX device to an appropriately rated branch circuit. See the label or nameplate affixed to your Dominion PX device for appropriate input ratings or range of ratings.
3. When a Dominion PX device powers up, it proceeds with the power-on self test and software loading for a few moments.
4. When the software has completed loading, the LED display illuminates.

Configuring Dominion PX

There are two alternatives to initially configure a Dominion PX device:

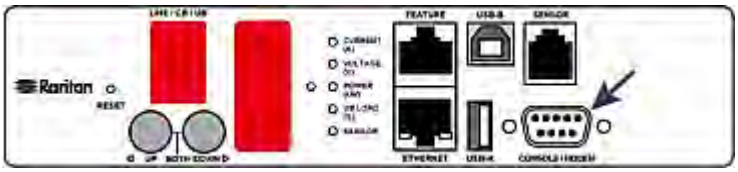
- Connect the Dominion PX device to a computer to configure it, using a serial connection between Dominion PX and the computer. The computer must have a communications program such as HyperTerminal or PuTTY. In addition, you need a null-modem cable with DB9 connectors on both ends (Raritan part number: 254-01-0006-00).
- Connect the Dominion PX device to a TCP/IP network that supports DHCP. A Category 5e/6 UTP cable is required.

Tip: The DHCP-assigned IP address of the PDU can be retrieved through the PDU's MAC address. You can contact your LAN administrator for assistance. See **MAC Addresses** *(see "***MAC Address***" on page 228).*

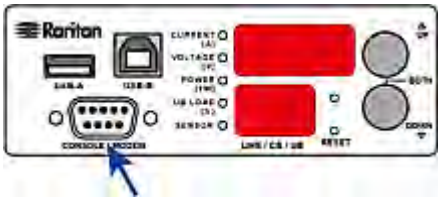
Connecting the PDU to a Computer

To configure Dominion PX using a computer, it must be connected to the computer with an RS-232 serial interface.

See this diagram for the serial port location on Zero U models.



See this diagram for the serial port location on 1U modelss.



To connect Dominion PX to a computer via a null-modem cable:

1. Connect one end of the null-modem cable to the RS-232 port labeled CONSOLE / MODEM on the Dominion PX device.
2. Connect the other end of the null-modem cable to the serial port (COM) on the computer.

Note: If you plan to use the serial connection to log in to the command line interface, leave the cable connected after the configuration is complete.

Connecting Dominion PX to Your Network

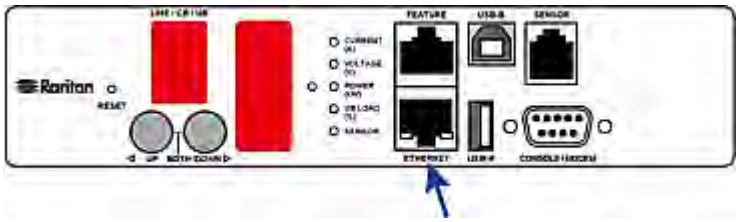
To use the web interface to administer Dominion PX, you must connect the Dominion PX device to your local area network (LAN). Dominion PX can be connected to a wired or wireless network.

Note: If your PDU is not implemented with the wireless networking feature, then make a wired connection.

To make a wired connection:

1. Connect a standard Category 5e/6 UTP cable to the ETHERNET port on the Dominion PX device.
2. Connect the other end of the cable to your LAN.

See the diagram for the ETHERNET port location on Zero U models.



For 1U models, the ETHERNET port is located on the back. See the diagram for the port location.

To make a wireless connection:

Do one of the following:

- Plug a 802.11n wireless USB LAN adapter into the USB-A port on your Dominion PX device.
- Connect a USB docking station to the USB-A port on the Dominion PX device and plug the 802.11n wireless USB LAN adapter into the appropriate USB port on the docking station.

Supported Wireless LAN Configuration

If you select the wireless connection, ensure that both of your wireless USB LAN adapter and wireless network configuration meet the following requirements.

- Network type: 802.11n
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK
- Encryption: CCMP (AES)

Important: Currently only Raritan-provided wireless USB LAN adapters are supported. You may contact Raritan Technical Support for this information.

Initial Network Configuration

After the Dominion PX device is connected to your network, you must provide it with an IP address and some additional networking information.

This section describes the initial configuration via a serial connection only.

Note: To configure Dominion PX via the LAN, see **Using the Web Interface** *(on page 37) for using the web interface.*

To configure Dominion PX:

1. Go to the computer that you connected to the Dominion PX device and open a communications program such as HyperTerminal or PuTTY.
2. Select the appropriate serial port, and make sure the port settings are configured as follows:
   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None
3. Press Enter.
4. Dominion PX prompts you to log in. Note that both of user name and password are case sensitive.
   a. At the Username prompt, type `admin` and press Enter.
   b. At the Password prompt, type `raritan` and press Enter.
5. You are prompted to change the password if this is the first time you log in to the Dominion PX device. Follow the onscreen instructions to type your new password.
6. The # prompt appears when you log in successfully.
7. Type `config` and press Enter. The config:# prompt appears, indicating that you have entered the configuration mode.

   ```
   config:# _
   ```

8. To configure network settings, type appropriate commands, and press Enter. All commands are case sensitive so make sure you capitalize them correctly.
   a. To set the networking mode, type this command:

   `networkingMode <mode>`

   where <mode> is either *wired* for wired connection (default) or *wireless* for wireless connection.

b. If you select the wireless network mode in the previous step, you should set the Service Set Identifier (SSID), Pre-Shared Key (PSK) and Basic Service Set Identifier (BSSID).

To set	Use this command
SSID	`wireless SSID <ssid>` where <ssid> is the SSID string.
PSK	`wireless PSK <psk>` where <psk> is the PSK string.
BSSID	`wireless BSSID <bssid>` where <bssid> is the AP MAC address.

Tip: You can combine all commands to configure all wireless parameters at a time. The command syntax is like this: `wireless SSID <ssid> PSK <psk> BSSID <bssid>`.

c. To set the IP configuration method, type this command:

`network ipConfigurationMode <mode>`

where <mode> is either *dhcp* for auto configuration (default) or *static* for specifying a static IP address.

d. To configure IP and other network parameters, use the commands shown in either table.

- If you chose "dhcp" in Step c, you may use this command.

To set	Use this command
Preferred host name (optional)	`network preferredHostName <name>` where <name> is the preferred host name.

- If you chose "static" in Step c, use the following commands for setting up static-IP-related parameters.

To set	Use this command
Static IP address	`network ipAddress <ip address>` where <ip address> is the IP address you want to assign.
Subnet mask	`network subnetMask <netmask>` where <netmask> is the subnet mask.
Gateway	`network gateway <ip address>` where <ip address> is the IP address of the gateway.
Primary DNS server	`network primaryDNSServer <ip address>` where <ip address> is the IP address of the primary DNS server.
Secondary DNS server (optional)	`network secondaryDNSServer <ip address>` where <ip address> is the IP address of the secondary DNS server.

e. The default LAN interface speed "auto" works in most of scenarios and should not be changed unless necessary. To change it, use this command:

`network LANInterfaceSpeed <option>`

where <option> is one of the options: auto, 10Mbps, or 100Mbps.

f. The default duplex mode "auto" works in most of scenarios and should not be changed unless necessary. To change it, type this command:

`network LANInterfaceDuplexMode <mode>`

where <mode> is one of the options: half, full, or auto.

9. To quit the configuration mode with or without saving the changes, type either command, and press Enter.

Command	Description
`apply`	Save all configuration changes and quit the configuration mode.
`cancel`	Abort all configuration changes and quit the configuration mode.

The # prompt appears, indicating that you have quit the configuration mode.

10. To verify whether all settings are correct, type the following commands one by one. Current network settings are displayed.

Command	Description
`show networkingMode`	Show current networking mode.
`show network details`	Show all network parameters.
`show wireless details`	Show all wireless parameters. (Perform this command only when you enable the wireless mode.)

Tip: You can also type "`show network`" and "`show wireless`" to display a shortened version of network settings.

11. If all are correct, type `exit` to log out of Dominion PX. If any are incorrect, repeat Steps 7 to 10 to change any network settings.

The IP address configured may take seconds to take effect.

Connecting Environmental Sensors (Optional)

To enable Dominion PX to detect environmental conditions, connect one or more Raritan environmental sensors to the Dominion PX device.

The maximum distance for all sensor cabling plugged into the product's sensor port should not exceed 30 meters/100 feet. Contact Raritan Technical Support if you have questions.

You can connect up to 16 environmental sensors to a Dominion PX device by using a Raritan sensor hub.

A DPX-T2H2 counts as 4 sensors. A DPX-T3H1 counts as 4 sensors.

Warning: For proper operation, wait for 15~30 seconds between each connection operation or each disconnection operation of environmental sensors.

To directly connect one or multiple environmental sensors:

- Plug the connector of the environmental sensor into the SENSOR port on your Dominion PX device.

  Note: Depending on the model you purchased, the number of SENSOR ports varies.

To connect environmental sensors via an optional PX sensor hub:

1. Connect a Raritan sensor hub to the Dominion PX device.
   a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.
   b. Plug the other end into the SENSOR port on the Dominion PX device.
2. Connect Raritan environmental sensors to any of the four OUT ports on the hub.

Raritan sensor hubs CANNOT be cascaded so at most a sensor hub can be connected to each SENSOR port on the Dominion PX device. This diagram illustrates a configuration with a sensor hub connected.

❶	Dominion PX device
❷	Raritan-provided phone cable
❸	Raritan PX sensor hub
❹	Raritan environmental sensors

About Contact Closure Sensors

Raritan's contact closure sensor (DPX-CC2-TR) can detect the open-and-closed status of the connected detectors/switches. It requires the integration of at least a discrete (on/off) detector/switch to work properly. The types of discrete detectors/switches that can be plugged into DPX-CC2-TR include those for:

- Door open/closed detection
- Door lock detection
- Floor water detection
- Smoke detection
- Vibration detection

Raritan does NOT provide these discrete detectors/switches. They are third-party probes so you must test them with Raritan's DPX-CC2-TR to ensure they work properly.

Integration and testing for third-party detectors/switches is the sole responsibility of the customer. Raritan cannot assume any liability as a result of improper termination or failure (incidental or consequential) of third-party detectors/switches that customers provide and install. Failure to follow installation and configuration instructions can result in false alarms or no alarms. Raritan makes no statement or claim that all third-party detectors/switches will work with DPX-CC2-TR.

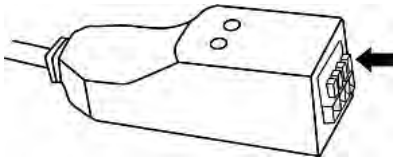
Connecting Third-Party Detectors/Switches to DPX-CC2-TR

A DPX-CC2-TR unit provides two channels for connecting two third-party detectors/switches. There are four spring-loaded termination points on the body of DPX-CC2-TR: the two to the right are associated with one channel (as indicated by the LED number), and the two to the left are associated with another channel. You must plug the third-party detectors/switches into these termination points.

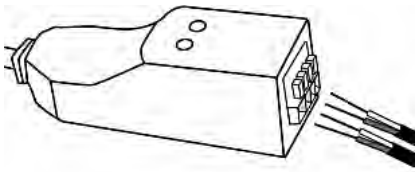
To connect third-party detectors/switches:

1. Strip the insulation around 12mm from the end of each wire of two third-party detectors/switches.
2. Press and hold down the tiny rectangular buttons above the termination points on the body of DPX-CC2-TR.

Note: Each button controls the spring of each corresponding termination point.



3. Fully insert each wire of both third-party detectors/switches into each termination point.
   - Plug both wires of a detector/switch into the two termination points to the left.
   - Plug both wires of another detector/switch into the two termination points to the right.



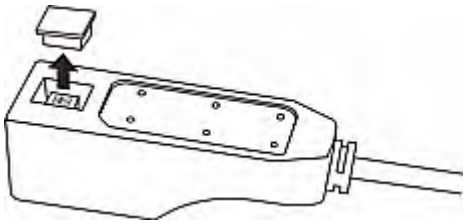
4. Release the tiny rectangular buttons after inserting four wires into four termination points.
5. Verify that these wires are firmly fastened.

Configuring a Contact Closure Sensor

Before using DPX-CC2-TR to detect the contact closure status, water, smoke or vibration, you must determine the normal state by adjusting its dip switch, which controls the LED state on the body of DPX-CC2-TR. A dip switch is associated with a channel.

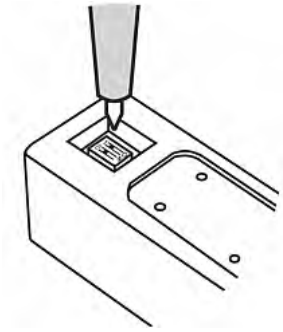
To adjust the dip switch setting:

1. Place the detectors/switches connected to DPX-CC2-TR to the position where you want to detect a specific environmental situation.
2. Uncover the dip switch on the body of DPX-CC2-TR.



3. To set the Normal state for channel 1, locate the dip switch labeled 1.
4. Use a pointed tip such as a pen to move the slide switch to the end labeled NO (Normally Open) or NC (Normally Closed).

- Normally Open: The open status of the connected detector/switch is considered normal.
- Normally Closed: The closed status of the connected detector/switch is considered normal. This is the default.



5. To set the Normal state for channel 2, repeat Step 4 for adjusting the other dip switch's setting.
6. Install back the dip switch cover.

Note: The dip switch setting must be properly configured, or the sensor LED may be incorrectly lit when in the Normal state.

Contact Closure Sensor LEDs

DPX-CC2-TR is equipped with the LEDs for showing the state of the connected detectors/switches.

The LED is lit when the associated detector/switch is in the "abnormal" state, which is the opposite of the Normal state. See ***Configuring a Contact Closure Sensor*** (on page 23) for how to set the Normal state.

The meaning of a lit LED varies depending on the Normal state settings.

- **When the Normal state is set to Closed:**

LED	Sensor state
Not lit	Closed
Lit	Open

- **When the Normal state is set to Open:**

LED	Sensor state
Not lit	Open
Lit	Closed

Connecting the Asset Management Sensor (Optional)

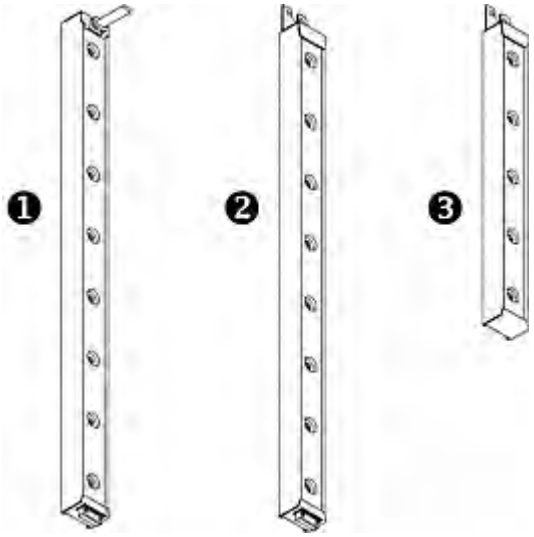
You can remotely track the locations of up to 48 IT devices in the rack by connecting an asset management sensor (asset sensor) to the Dominion PX device after these IT devices are tagged electronically.

To use this asset management feature, you need the following items:

- Raritan asset sensors: An asset sensor transmits the tagging and positioning information to the Dominion PX device.
- Raritan asset tags: An asset tag electronically tags the IT device where it is attached.

Attaching Asset Sensors to a Rack

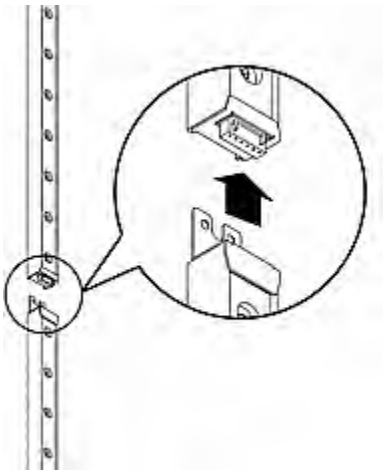
Each tag port on the asset sensors corresponds to a rack unit and can be used to locate the IT devices on a specific rack (or cabinet). For each rack, you can attach up to 6 asset sensors, consisting of one MASTER and five SLAVE asset sensors.



Number	Item
❶	8U MASTER asset sensor with 8 tag ports
❷	8U SLAVE asset sensor with 8 tag ports
❸	5U SLAVE asset sensor with 5 tag ports

To attach asset sensors to a rack:

1. Connect a MASTER asset sensor to an 8U SLAVE asset sensor.



- Plug the white male DIN connector of the slave asset sensor into the white female DIN connector of the master asset sensor.
- Make sure that the U-shaped sheet metal adjacent to the male DIN connector is inserted into the rear slot of the master asset sensor. It is recommended to screw up the U-shaped sheet metal to reinforce the connection.

2. Connect another 8U slave asset sensor to the one being attached to the master asset sensor in the same manner as Step 1.
3. Repeat Step 2 to connect more slave asset sensors. The maximum length of the combined asset sensors can be 45U or 48U.
   - The final asset sensor can be 8U or 5U, depending on the height of your rack.
4. Vertically attach the asset sensor assembly to the rack, next to the IT equipment, making each tag port on the asset sensor horizontally align with an IT device on the rack. The asset sensors are automatically attracted to the rack because of magnetic stripes on the back.

Connecting Asset Sensors to Dominion PX

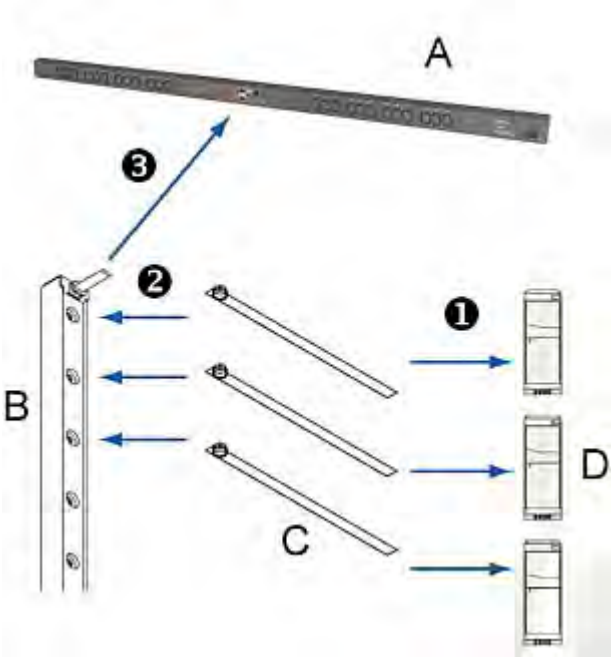
You need both of asset sensors and asset tags for tracking IT devices. Asset tags, which are affixed to IT devices, provide an ID for each IT device, while the asset sensors transmit ID and positioning information to the Dominion PX device.

To connect asset sensors to Dominion PX:

1. Affix an asset tag to each IT device through the tape on the tag's back.
2. Plug the connector on each asset tag into the corresponding tag port on the asset sensor.

3. Connect the asset sensor on the rack to the Dominion PX device by following this procedure:
   a. Connect one end of a Category 5e/6 cable to the RJ-45 connector on the MASTER asset sensor.
   b. Connect the other end of the cable to the FEATURE port on the Dominion PX device.

      The Dominion PX device supplies power to asset sensors through the Category 5e/6 cable.



Letter	Item
A	Dominion PX device
B	Asset sensors
C	Asset tags
D	IT devices, such as servers

Note: The PDU cannot detect how many rack units the connected asset sensor(s) support. You must provide the information to the PDU manually. See ***Configuring the Asset Sensor*** (on page 122).

Chapter 4 Using the PDU

This chapter explains how to use the Dominion PX device. It describes the LEDs and ports on the PDU, and explains how to use the LED display panel. It also explains how the circuit breaker (overcurrent protector) works and when the beeper sounds.

In This Chapter

Panel Components

Dominion PX comes in Zero U, 1U, and 2U sizes. All types of models come with the following components on the outer panels.

- Power cord
- Outlets
- Connection ports
- LED display
- Reset button

Power Cord

Most of Raritan PDUs come with an installed power cord, which is ready to be plugged into an appropriate receptacle for receiving electricity. Such devices cannot be rewired by the user.

Connect each Dominion PX device to an appropriately rated branch circuit. See the label or nameplate affixed to your Dominion PX device for appropriate input ratings or range of ratings.

There is no power switch on the Dominion PX device. To power cycle the PDU, unplug it from the branch circuit, wait 10 seconds and then plug it back in.

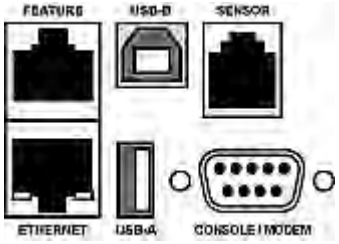
Outlets

The number of outlets varies from model to model. PX-1000 series products are not implemented with the outlet switching feature so all outlets are always in the ON state.

Connection Ports

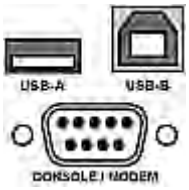
Depending on the model you purchased, the number of ports available varies.

- For most of Zero U models, there are 6 ports located on the front panel as shown below.

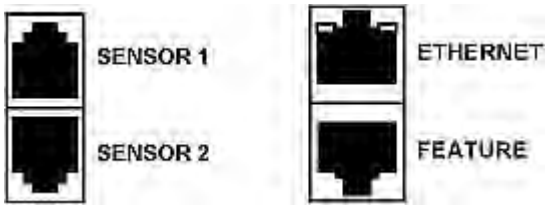


- For 1U models, there are 7 ports located on front and back panels respectively.

  - Front panel ports:



  - Back panel ports:



The port difference between Zero U and 1U models is that Zero U models provide only one sensor port while 1U models provide two sensor ports.

The table below explains the function of each port.

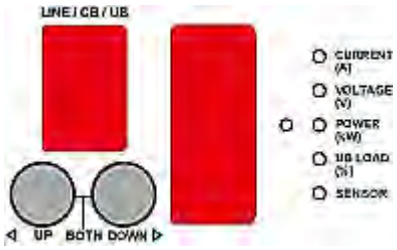
Port	Used for...
USB-B	Establishing a USB connection between a computer and the Dominion PX device. This port is reserved for a future release.
USB-A	Connecting a USB device. This is a "host" port, which is powered, per USB 2.0 specifications.

Port	Used for...
FEATURE	Connection to some Raritan access products (such as Dominion KX II) through the use of a power CIM, OR -- Connection to a Raritan Asset Management Sensor, which allows you to track the locations of the IT devices in the rack. See ***Connecting the Asset Management Sensor (Optional)*** (on page 25). *Warning: This is not an RS-232 port so do NOT plug in an RS-232 device, or damages can be caused to the device.*
CONSOLE/ MODEM	Establishing a serial connection between a computer and the Dominion PX device: This is a standard DTE RS-232 port. You can use a null-modem cable with two DB9 connectors on both ends to connect Dominion PX to the computer.
SENSOR	Connection to Raritan's environmental sensors. For Zero U products, a sensor hub is required if you want to connect more than one environmental sensor.
ETHERNET	Connecting the Dominion PX device to your company's network: Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the Dominion PX device remotely using the web interface. There are two small LEDs adjacent to the port: ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds.

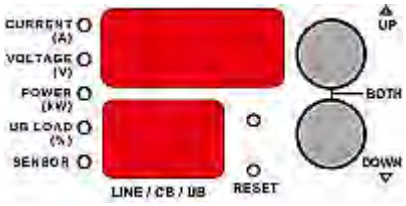
LED Display

The LED display is located on the side where outlets are available. The following picture shows the LED display.

The diagram shows the LED display on Zero U models.



The diagram shows the LED display on 1U models.



The LED display consists of:

- A row displaying three digits
- A row displaying two digits
- Up and Down buttons
- Five LEDs for measurement units

Note: When a Dominion PX device powers up, it proceeds with the power-on self test and software loading for a few moments. When the software has completed loading, the LED display illuminates.

Three-Digit Row

The three-digit row shows the readings for the selected component. Values that may appear include:

- Current of the selected circuit breaker
- Active power or unbalanced load of the inlet
- Current, voltage, or active power of the selected line

Note: L1 voltage refers to the L1-L2 or L1-N voltage, L2 voltage refers to the L2-L3 or L2-N voltage, and L3 voltage refers to the L3-L1 or L3-N voltage.

- The text “FuP,” which indicates that the **F**irmware **uP**grade is being performed
- The text "CbE," which indicates the selected circuit breaker has tripped

LEDs for Measurement Units

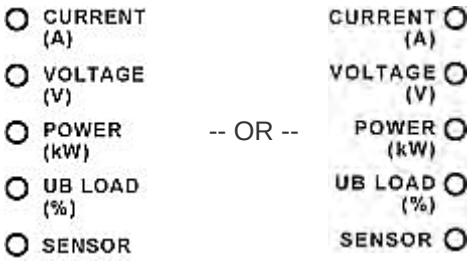
Five small LED indicators are adjacent to the three-digit row: four measurement units LEDs and one Sensor LED.

The measurement units vary according to the readings that appear in the three-digit row. They are:

- Amp (A) for current
- Volt (V) for voltage
- Kilowatt (kW) for active power
- Unbalanced load (%)

One of the measurement unit LEDs will be lit to indicate the unit for the value currently shown in the three-digit row.

The Sensor LED is lit only when Dominion PX detects the physical connection of any environmental sensor.



Two-Digit Row

The two-digit row shows the number of the currently selected line or circuit breaker. Values that may appear include:

- Cx: This indicates the selected circuit breaker, where x is the circuit breaker number. For example, C1 represents Circuit Breaker 1.
- n: This indicates the neutral line on a three-phase Y-wired PDU.
- Lx: This indicates the selected line of a single-inlet PDU, where x is the line number. For example, L2 represents Line 2.

Note: For a single-phase model, L1 current represents the Unit Current.

- AP: This indicates the selected inlet's active power.
- UL: This represents the selected inlet or outlet's **U**nbalanced **L**oad, which is only available for a three-phase PDU.

During the firmware upgrade, some Dominion PX models may show bx in the two-digit row to indicate the relay or meter board numbered x is being updated.

Automatic Mode

When left alone, the LED display cycles through the line readings and circuit breaker readings at intervals of 10 seconds, as available for your Dominion PX. This is the Automatic Mode.

Manual Mode

You can press the Up or Down button to enter the Manual Mode so that a particular line or circuit breaker can be selected to show specific readings.

To operate the LED display:

1. Press the Up or Down button until the desired line or circuit breaker number is selected in the two-digit row. Or you can press either button to select the inlet's active power, which is shown as *AP*.
   - Pressing the △ (UP) button moves up one selection.
   - Pressing the ▽ (DOWN) button moves down one selection.
2. Current of the selected component is shown in the three-digit row. Simultaneously the CURRENT(A) LED is lit. See ***LEDs for Measurement Units*** (on page 32).
3. When selecting a line, you can press the Up and Down buttons simultaneously to switch between voltage, active power and current readings.
   - The voltage appears in this format: XXX (V). It is displayed for about five seconds, after which the current reading re-appears. When the voltage is displayed, the VOLTAGE(V) LED is lit.
   - The active power appears in one of the formats: X.XX, XX.X, and XXX (kW). It is displayed for about five seconds, after which the current reading re-appears. When the active power is displayed, the POWER(kW) LED is lit.
4. When selecting the inlet (AP), it displays the active power reading.
   - The active power appears in one of the formats: X.XX, XX.X, and XXX (kW). When the active power is displayed, the POWER(kW) LED is lit.

Note: The LED display returns to the Automatic Mode after 20 seconds elapse since the last time any button was pressed.

Note: A few Dominion PX models may show some current being drawn or power consumption while no loads are physically attached to the PDU. For details, see **Non-Zero Readings While No Loads Attached** *(on page 240).*

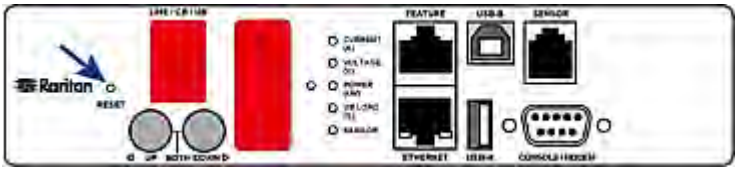
Reset Button

The reset button is located inside the small hole near the two-digit row.

The Dominion PX device can be reset to its factory default values using this button when a serial connection is available. See ***Resetting to Factory Defaults*** (on page 237).

Without the serial connection, pressing this reset button restarts the Dominion PX device's software without any loss of power to outlets. This operation also power cycles the LED display, causing the LED display to go blank and then return to normal.

The following images indicate the location of the reset button.



Circuit Breakers

Dominion PX models rated over 20A (North American) or 16A (international) contain branch circuit breakers. These circuit breakers automatically trip (disconnect power) when the current flowing through the circuit breaker exceeds its rating.

When a circuit breaker trips, power flow ceases to all outlets connected to it. You must manually reset the circuit breaker so that affected outlets can resume normal operation.

Depending on the model you purchased, the circuit breaker may use a button- or handle-reset mechanism.

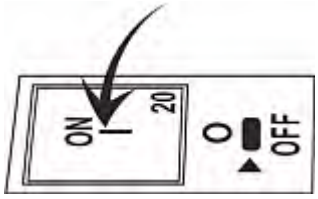
Resetting the Button-Type Circuit Breaker

Your button-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

To reset the button-type breakers:

1. Locate the breaker whose ON button is up, indicating the breaker has tripped.

2. Examine your Dominion PX device and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**
3. Press the ON button until it is completely down.

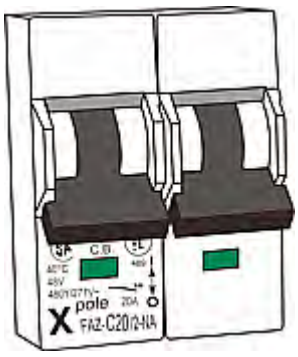


Resetting the Handle-Type Circuit Breaker

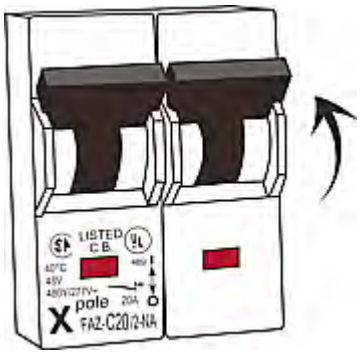
Your handle-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

To reset the handle-type breakers:

1. Lift the hinged cover over the breaker.
2. Check if the colorful rectangle or triangle below the operating handle is GREEN, indicating the breaker has tripped.



3. Examine your Dominion PX device and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**
4. Pull up the operating handle until the colorful rectangle or triangle turns RED.



Beeper

Dominion PX includes a beeper to issue an audible alarm when a significant situation occurs.

- The beeper sounds an alarm within 3 seconds of a circuit breaker trip.
- The beeper stops as soon as all circuit breakers have been reset.

Chapter 5 Using the Web Interface

This chapter explains how to use the web interface to administer a Dominion PX device.

In This Chapter

Supported Web Browsers

The following web browsers can be used to access the Dominion PX web interface:

- Internet Explorer® 7 (IE7) and Internet Explorer® 8 (IE8)
- Firefox 3.n.n (where n represents a numeric digit)
- Safari, Konqueror

Note: IE6 and Chrome are NOT supported.

Logging in to the Web Interface

To log in to the web interface, you must enter a user name and password. The first time you log in to Dominion PX, use the default user name (admin) and password (raritan). You are then prompted to change the password for security purposes.

Exception: If you already changed the password for the admin account during the **Initial Network Configuration** *(on page 16), use the new password instead to log in to the web interface, and Dominion PX will NOT prompt you to change the password.*

After successfully logging in, you can create user profiles for your other users. These profiles define their login names and passwords. See ***Creating a User Profile*** (on page 64).

Login

The web interface allows a maximum of 16 users to log in simultaneously.

You must enable JavaScript in the web browser for proper operation.

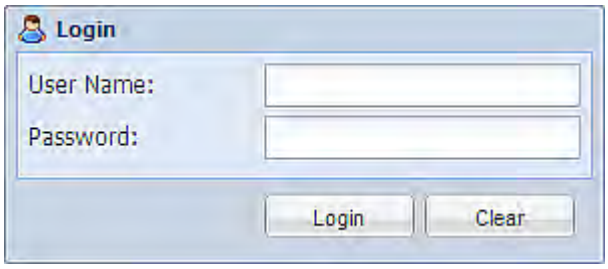
▶ **To log in to the web interface:**

1. Open a browser, such as Microsoft Internet Explorer or Mozilla Firefox, and type this URL:

   http(s)://<ip address>

   where *<ip address>* is the IP address of the Dominion PX device.

2. If any security alert message appears, click OK or Yes to accept. The Login page then opens.

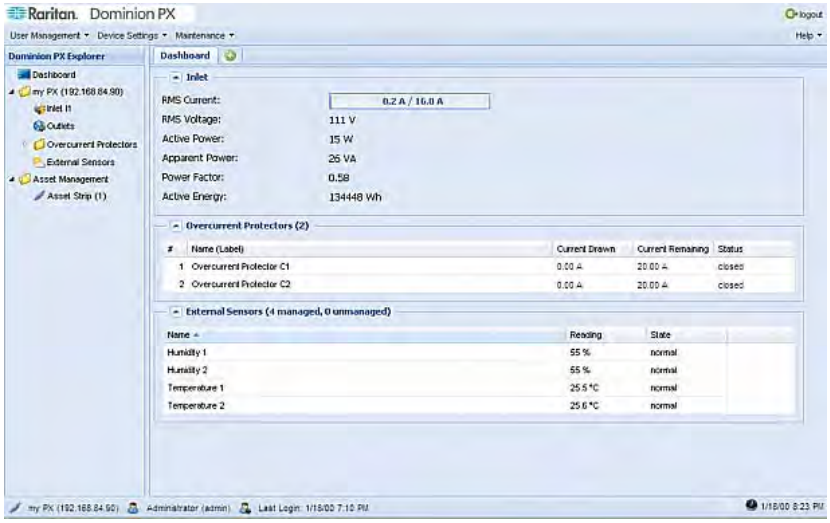


3. Type your user name in the User Name field, and password in the Password field.

   Note: Both the user name and password are case sensitive, so make sure you capitalize them correctly. If you typed them incorrectly, click Clear to clear either the inputs or any error message that appears.

4. Click Login or press Enter. The Dominion PX page opens.

Note: Depending on your hardware configuration, elements shown on the Dominion PX page may appear slightly different from this image.



Changing Your Password

Normal users can change their own passwords if they have the Change Own Password permission. See ***Setting Up Roles*** (on page 68, on page 69).

If you are the administrator (admin), the Dominion PX web interface automatically prompts you to change the password if this is your first time to log in to Dominion PX.

To change your password:

1. Choose User Management > Change Password. The Change User 'XXX' Password dialog appears, where XXX is the user's login name.

2. Type the current password in the Old Password field.
3. Type your new password in the Password and Confirm Password fields. The password can be 4 to 32 characters long. It is case sensitive.

4. Click OK to save the changes.

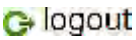
Tip: If you have the Administrator Privileges, you can change other users' passwords. See **Modifying a User Profile** *(on page 67).*

Logout

After finishing your tasks with Dominion PX, you should log out to prevent others from accessing the web interface.

To log out of the web interface:

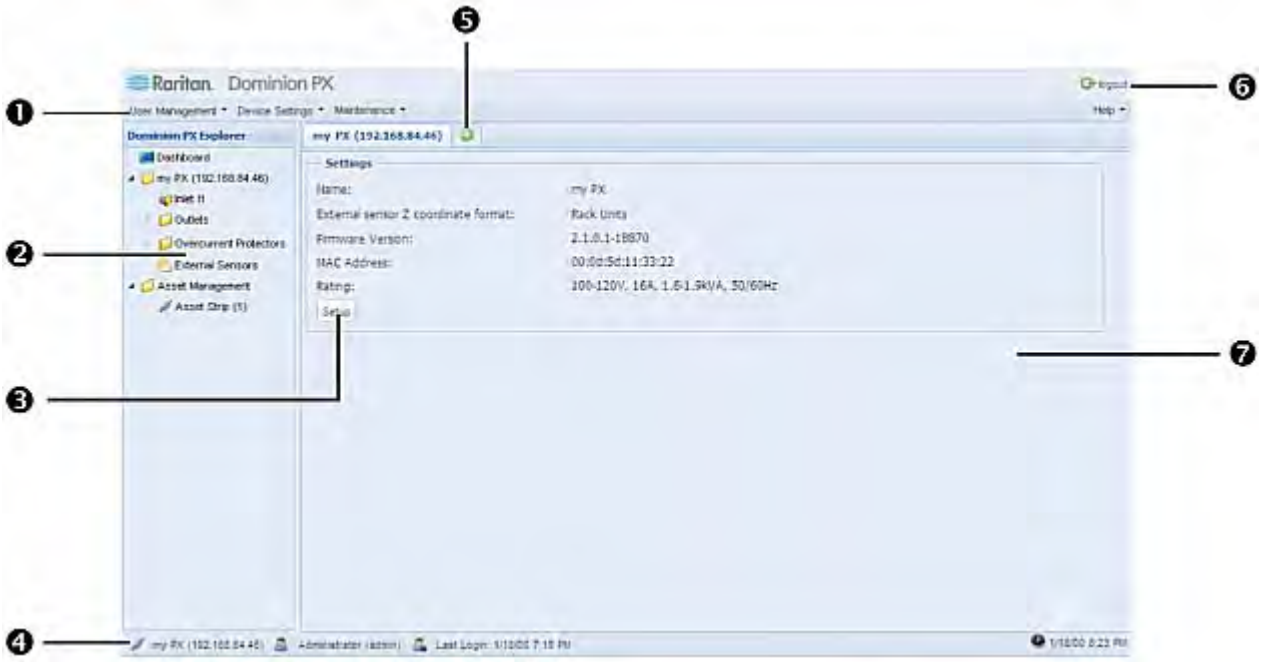
1. Do one of these:
   - Click "logout" on the top-right corner of the web interface.

   - Close the web browser by clicking the Close button () on the top-right corner of the browser.
   - Close the web browser by choosing File > Close, or File > Exit. The command varies according to the version of the browser you use.
   - Choose the Refresh command or click the Refresh button on the web browser.
2. Either the login page opens or the browser is closed, depending on your choice for Step 1.

Introduction to the Web Interface

The web interface provides two panes, a menu bar, a status bar, an Add Page icon, and a logout button throughout every page.



Number	Web interface element
❶	Menus
❷	Dominion PX Explorer pane
❸	Setup button*
❹	Status bar
❺	Add Page icon
❻	Logout button
❼	Data pane

* The Setup button is not available on some pages, such as the *Dashboard* page.

For detailed information about these web interface elements, see the sections that follow.

Menus

There is a menu bar across the top of the page. You can click any menu to select the desired menu item from the drop-down list.

Four menus are available for managing different tasks or showing information.

- **User Management** contains menu items for managing user profiles, permissions (roles), and password.
- **Device Settings** deals with device-related settings, such as the device name, network settings, security settings, and system time.
- **Maintenance** provides tools that are helpful for maintaining the Dominion PX device, such as the event log, hardware information, firmware upgrade and so on.
- **Help** displays information regarding the firmware and all open source packages embedded on the Dominion PX device. In addition, you can access the user guide from this menu.

Dominion PX Explorer Pane

The hierarchical tree to the left displays the Dominion PX device you are accessing as well as all physical components embedded on or connected to this PDU, such as inlets, outlets, and environmental sensors. In addition, an icon named Dashboard is available for displaying the PDU summary information.

The tree structure comprises three hierarchical levels.

First level	Second level	Third level
Dashboard	None	None
PDU folder*	Inlet I1	None
	Outlets	None
	Overcurrent Protectors folder	C1 to Cn**
	External Sensors	None
Asset Management	Asset Strip 1	None

* The PDU folder is named "my PX" by default. The name changes after customizing the device name. See ***Naming the PDU*** (on page 53).

** n represents the final number of that component.

To navigate through the tree:

1. To expand any folders, see ***Expanding the Tree*** (on page 43).

2. To show any tree item's data, click on that item. See ***Add Page Icon*** (on page 46).

Expanding the Tree

The icons representing all components implemented on or connected to the Dominion PX device are expanded by default. If they are hidden, you may expand the tree manually to show all component icons.

To expand the tree:

1. By default, the PDU folder has been expanded.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 53).*

   If it is not expanded, click the white arrow ▷ prior to the folder icon, or double-click the folder. The arrow then turns into a black, gradient arrow ◢, and icons of components or component groups appear below the PDU folder.

2. To expand any component group at the second level, click the white arrow ▷ prior to the folder icon, or double-click the folder.

   The arrow then turns into a black, gradient arrow ◢, and icons representing individual components appear below the group folder.

   Repeat Step 2 for other component groups you want to expand. The expanded tree looks similar to this image.

Collapsing the Tree

You can collapse the whole tree structure or a specific component group to hide all or partial tree items.

To collapse the whole tree:

- Click the black, gradient arrow ◢ prior to the PDU folder icon, or double-click the folder.

  Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 53).*

  The arrow then turns into a white arrow ▷, and all items below the PDU folder disappear.

To hide some tree items:

1. Click the black, gradient arrow ◢ prior to the component group folder that you want to collapse, or double-click the folder.

   The arrow then turns into a white arrow ▷, and all items below the folder disappear.

2. Repeat Step 1 for other component groups you want to collapse.

Adjusting the Pane

You can change the width of the pane to make the area larger or smaller.

To adjust the pane's width:

1. Move the mouse pointer to the right border of the Dominion PX Explorer pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

Setup Button

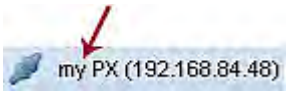
The Setup button is available for most tree items. It triggers a setup dialog where you can change settings for the selected tree item.

Status Bar

The status bar shows five pieces of information from left to right.

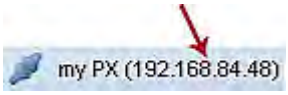
- *Device name:*

  This is the name assigned to the Dominion PX device. The default is "my PX." See ***Naming the PDU*** (on page 53).



- *IP address:*

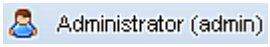
  The numbers enclosed in parentheses is the IP address assigned to the Dominion PX device. See ***Initial Network Configuration*** (on page 16) or ***Modifying the Network Settings*** (on page 54).



Tip: The presence of the device name and IP address in the status bar indicates the connection to the Dominion PX device. If the connection is lost, it shows " disconnected *" instead.*

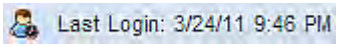
- *Login name:*

  This is the user name you used to log in to the web interface.



- *Last login time:*

  This shows the date and time this login name was used to log in to the device last time. When hovering the mouse pointer over the last login time, detailed information about the last login is displayed, including the access client and IP address.



- *System date and time:*

  Current date, year, and time are displayed to the right of the bar. If hovering the mouse pointer over the system date and time, the time zone information is also displayed.

Sometimes a flag icon ( ) may appear to the far right of the bar when a communication error between the Dominion PX device and the graphical user interface (GUI) occurs. When the icon appears, you can click the icon to view the communications log. See ***Viewing the Communication Log*** (on page 129).

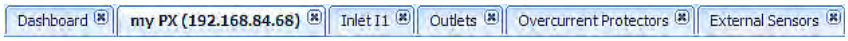
Add Page Icon

The Add Page icon  , located on the top of the data pane, lets you open data pages of multiple tree items without closing any opened page.

To open new data pages:

1. Click the Add Page icon  . A new tab along with a blank data page appears.
2. Click a tree item whose data page you want to open. The data of the selected tree item is then displayed on the blank data page.
3. To open more data pages, repeat Steps 1 to 2. All tabs representing opened pages are shown across the top of the page.

   The following diagram shows a multi-tab example.

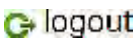


4. With multiple pages opened, you can take these actions:
   - To return to any previous data page, click the corresponding tab.

     If there are too many tabs to be all shown, two arrows ( and ) appear at the left and right borders of the pane. Click either or both arrows to navigate through all tabs.
   - To close any data page, click the Close button () in the corresponding tab.

Logout Button

Click the logout button when you want to log out of the web interface.



Data Pane

The right pane shows the data page of the selected tree item. The data page includes the item's current status, settings and a Setup button (if available).

The tab above the pane indicates the current selection of the data page.

You can change the width of the pane to make the area larger or smaller.

To adjust the pane's width:

1. Move the mouse pointer to the left border of the right pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

More Information

This section explains additional web interface elements or operations that are useful.

Warning Icon

If the value you entered in a specific field is invalid, a red warning icon appears to the right and the field in question is surrounded by a red frame as shown in this illustration.

When this occurs, hover your mouse pointer over the warning icon to view the reason and modify the entered value accordingly.

The Yellow- or Red-Highlighted Reading

When a numeric sensor's reading crosses any upper or lower threshold, the background color of the whole row turns to yellow or red for alerting users. If any circuit breaker trips, the circuit breaker's row is also highlighted in red.

See the table for the meaning of each color:

Color	State
White	The reading is between the lower and upper warning thresholds, or the reading is unavailable.
Yellow	The reading drops below the lower warning threshold or rises above the upper warning threshold.
Red	The meaning of the red color varies depending on the sensor type: ▪ For a numeric sensor, the color indicates the reading drops below the lower critical threshold or rises above the upper critical threshold. ▪ For circuit breaker trip sensor, it means the circuit breaker has tripped.

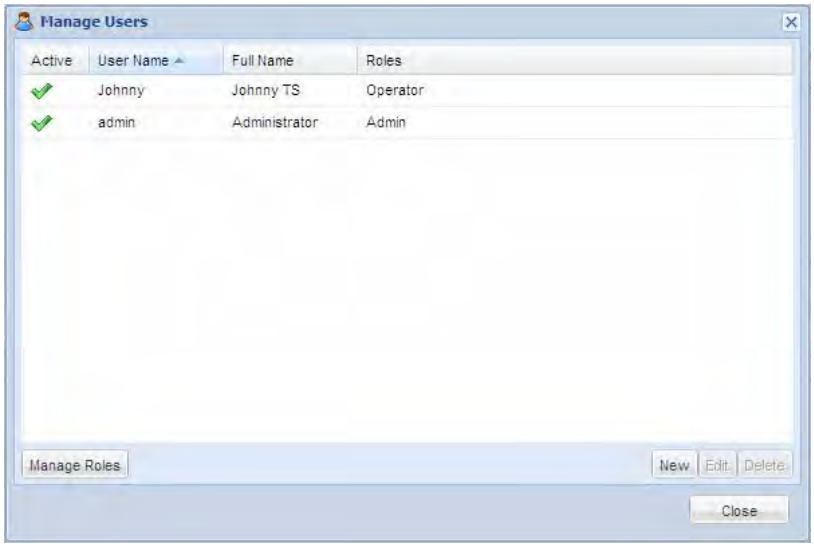
To find the exact meaning of the alert, read the information shown in the State (or Status) column of the same row:

- lower critical: The reading drops below the lower critical threshold.
- lower warning: The reading drops below the lower warning threshold.
- upper critical: The reading exceeds the upper critical threshold.
- upper warning: The reading exceeds the upper warning threshold.
- Open: The circuit breaker has tripped.

For information on the thresholds, see ***Setting Power Thresholds*** (on page 98).

Changing the View of a List

Some dialogs or data pages contain a list or table, such as the Manage Users dialog shown below. You may change the number of displayed columns or re-sort the list for better viewing the data. Note the column or sorting changes are not saved when quitting the dialog or data page. Next time when the dialog or page re-opens, the list returns to the default view.



Note: Not all dialogs support the sorting or column change functions.

Changing the Column

You can hide some columns of a list or table, or adjust a specific column's width.

To change displayed columns:

1. Hover your mouse pointer over any column header. A black triangle appears to the far right of this column header.

2. Click the black triangle, and a drop-down menu appears.
3. Point to Columns. A submenu showing all columns appears.
4. Click any column you want to deselect or select.
   - To hide a column, have its checkbox deselected.
   - To show a column, have its checkbox selected.

To change the column width:

1. Hover the mouse pointer to the right border of the desired column.
2. When the mouse pointer turns to a two-way arrow, drag the border horizontally to widen or shrink the column.

Changing the Sorting

By default, a list or table is sorted against the first column in the ascending order. You can re-sort the list in a reverse order or against a different column.

To re-sort the list by doing either of the following:

- Click the column header against which you want to sort the list.
  a. The first click sorts the list in the ascending order, indicated by a blue upward-pointing triangle .
  b. The second click reverses the sorting to the descending order, indicated by a blue downward-pointing triangle .
- Select a sorting command from the column menu.
  a. Hover your mouse pointer over the column header against which you want to sort the list. A black triangle appears to the far right of this column header.
  b. Click the black triangle, and a drop-down menu appears.
  c. Select Sort Ascending or Sort Descending.

The newly selected column header is marked with the upward- or downward-pointing triangle.

Resizing a Dialog

Most dialogs cannot be resized except for a few ones (such as the Event Log dialog), which can be resized to display more information at a time.

To resize a dialog:

1. Hover your mouse pointer over any border of the dialog.
2. When the mouse pointer turns to a double-headed arrow, drag the border vertically or horizontally to make the dialog bigger or smaller.

Browser-Defined Shortcut Menu

A shortcut menu, which is built in the web browser, may appear when right-clicking anywhere in the Dominion PX web interface.

The shortcut menu functions are defined by the browser. For example, the Back command on the Internet Explorer® (IE) shortcut menu works the same as the Back button in the IE browser. Both of these functions take you to the previous page.

For information on each shortcut menu command or item, see the online help or documentation accompanying your web browser.

Below is the illustration of the IE browser's shortcut menu. Available menu commands or items may slightly differ based on your web browser version.

Viewing the Dashboard

When you log in to the web interface, the Dashboard page is displayed by default. This page provides an overview of the Dominion PX device's status.

The page is divided into various sections according to the component type, such as inlet and circuit breakers.

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or the circuit breaker has tripped. See **The Yellow- or Red-Highlighted Reading** *(on page 47).*

After clicking any other icon in the hierarchical tree, the Dashboard page is overridden. To return to the Dashboard page, click the Dashboard icon.

When the Dashboard page is opened, you can do the following to uncover or hide specific data.

To collapse any section:

1. Locate the section you want to collapse.
2. Click the upward arrow prior to the section title. The data specific to the section is hidden.

To expand a collapsed section:

1. Locate the section you want to expand.
2. Click the downward arrow prior to the section title. The data specific to the section appears.

Device Management

Using the web interface, you can retrieve basic hardware and software information, give Dominion PX a new device name, set the system date and time, and modify network settings that were entered during the initial configuration process.

Displaying the PDU Information

To display information specific to the Dominion PX device that you are using, such as inlet or outlet types, trigger the Device Information dialog.

To display the PDU-specific information:

1. Choose Maintenance > Device Information. The Device Information dialog appears.

2. Click the tab containing the information you want to view. The number of available tabs varies according to the model you purchased.

Tab	Data
Device Information	General PDU information, such as model name, serial number, firmware version, hardware revision, and so on.
Outlets	Each outlet's receptacle type, operating voltage and rated current.
Inlets	Each inlet's plug type, rated voltage and current.
Overcurrent Protectors	Each circuit breaker's type, rated current and the outlets that it protects.
Controllers	Each inlet or outlet controller's serial number, firmware and hardware version.

Tab	Data
Asset Strips	The connected asset sensor's hardware ID, boot version, application version and protocol version.

Note: An outlet's operating voltage is derived from the inlet's rated voltage. The result of this calculation is rounded off mathematically to the nearest integer in volt. For example, if the calculation for the minimum voltage is 380/sqrt(3)=219.39 , the web interface displays 219 V.

3. Enlarge the dialog if necessary. See ***Resizing a Dialog*** (on page 49).
4. You can re-sort the list or change the columns displayed. See ***Changing the View of a List*** (on page 48).
5. Click Close to quit the dialog.

Tip: The firmware version is also available by clicking the PDU folder in the Dominion PX Explorer pane.

Naming the PDU

The default name for Dominion PX is *my PX*. You may give it a unique device name.

To change the device name:

1. Click the PDU folder.

Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 53).*

2. Click Setup. The Pdu Setup dialog appears.
3. Type a new name in the Device Name field.
4. Click OK to save the changes.

Modifying the Network Configuration

The network settings you can change via the web interface include IPv4, wired and wireless settings.

Modifying the Network Settings

Dominion PX was configured for network connectivity during the installation and configuration process. See ***Configuring Dominion PX*** (on page 13). If necessary, you can modify any network settings using the web interface.

To modify the IPv4 settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Locate the IPv4 Configuration section.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
DHCP	To auto-configure Dominion PX, select DHCP. With DHCP selected, you can enter a preferred DHCP host name, which is optional. Type the host name in the Preferred Hostname field. The host name: ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.
Static	To manually assign an IP address, select Static, and enter the following information in the corresponding fields: ▪ IP address ▪ Netmask ▪ Gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional)

4. Click OK to save the changes.

Role of a DNS Server

As Internet communications are carried out on the basis of IP addresses, appropriate DNS server settings are required for mapping domain names (host names) to corresponding IP addresses, or Dominion PX may fail to connect to the given host.

Therefore, DNS server settings are important for LDAP authentication. With appropriate DNS settings, Dominion PX can resolve the LDAP server's name to an IP address for establishing a connection. If the *SSL encryption* is enabled, the DNS server settings become critical since only fully qualified domain name can be used for specifying the LDAP server.

For information on LDAP authentication, see ***Setting Up LDAP Authentication*** (on page 88).

Modifying the Network Interface Settings

Dominion PX supports two types of network interfaces: wired and wireless. You should configure the network interface settings according to the networking mode that applies. See Connecting Dominion PX to Your Network.

Wired Network Settings

The LAN interface speed and duplex mode were set during the installation and configuration process. See ***Initial Network Configuration*** (on page 16).

By default, the LAN speed and duplex mode are set to "Auto" (automatic), which works in nearly all scenarios. You can change them if there are special local requirements.

To modify the network interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Locate the Interface Settings section.
3. In the Network Interface field, click the drop-down arrow, and select Wired from the list.
4. To change the LAN speed, click the drop-down arrow in the Speed field and select an option from the list.
   - Auto: System determines the optimum LAN speed through auto-negotiation.
   - 10 Mbit/s: The LAN speed is always 10 Mbps.
   - 100 Mbit/s: The LAN speed is always 100 Mbps.
5. To change the duplex mode, click the drop-down arrow in the Duplex field and select an option from the list.

- Auto: Dominion PX selects the optimum transmission mode through auto-negotiation.
- Full: Data is transmitted in both directions simultaneously.
- Half: Data is transmitted in one direction (to or from the Dominion PX device) at a time.

6. Click OK to save the changes.

Tip: You can check the LAN status in the Current State field, including the speed and duplex mode.

Wireless Network Settings

Wireless SSID, PSK and BSSID parameters were set during the installation and configuration process. See ***Initial Network Configuration*** (on page 16). You can change them via the web interface.

To modify the wireless interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Locate the Interface Settings section.
3. In the Network Interface field, click the drop-down arrow, and select Wireless from the list.
4. Check the Hardware State field to ensure that the Dominion PX device has detected the wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported. See Connecting Dominion PX to Your Network.
5. Type the name of the wireless access point (AP) in the SSID field.
6. Type the PSK string in the Pre-Shared Key field.
7. If the BSSID is available, select the Force AP BSSID checkbox, and type the MAC address in the BSSID field.

   Note: BSSID refers to the MAC address of an access point in the wireless network.

8. Click OK to save the changes.

Modifying the Network Service Settings

Dominion PX supports these network communication services: HTTPS, HTTP, Telnet and SSH.

HTTPS and HTTP enable the access to the web interface, and Telnet and SSH enable the access to the ***command line interface*** (see "***Using the Command Line Interface***" on page 142).

By default, SSH is enabled, Telnet is disabled, and all TCP ports for supported services are set to standard ports. You can change default settings if necessary.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure.

In addition, Dominion PX also supports SNMP protocol.

Changing the HTTP(S) Settings

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the Dominion PX device so it is a more secure protocol than HTTP.

By default, any access to Dominion PX via HTTP is automatically redirected to HTTPS. See ***Forcing HTTPS Encryption*** (on page 72).

To change the HTTP or HTTPS port settings:

1. Choose Device Settings > Network Services > HTTP. The HTTP Settings dialog appears.
2. To use a different port for HTTP or HTTPS, type a new port number in the corresponding field. Valid range is 1 to 65535.

   Warning: Different network services cannot share the same TCP port.
3. Click OK to save the changes.

Changing the SSH Settings

You can enable or disable the SSH access to the command line interface, or change the default TCP port for the SSH service.

To change the SSH service settings:

1. Choose Device Settings > Network Services > SSH. The SSH Settings dialog appears.
2. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
3. To enable the SSH application, select the Enable SSH Access checkbox. To disable it, deselect the checkbox.

4. Click OK to save the changes.

Changing the Telnet Settings

You can enable or disable the Telnet access to the command line interface, or change the default TCP port for the Telnet service.

To change the Telnet service settings:

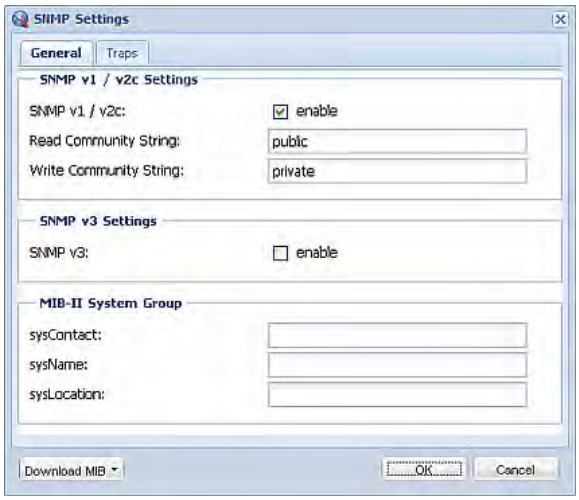
1. Choose Device Settings > Network Services > Telnet. The Telnet Settings dialog appears.
2. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
3. To enable the Telnet application, select the Enable Telnet Access checkbox. To disable it, deselect the checkbox.
4. Click OK to save the changes.

Configuring the SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the Dominion PX device. Enabling SNMP communication allows Dominion PX to send SNMP trap events to the manager, as well as allows the manager to retrieve and control the power status of each outlet.

To configure the SNMP communication:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.

- Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
- Type the read/write community string in the Write Community String field. Usually the string is "private."

3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

Tip: You can permit or disallow a user to access Dominion PX via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 137).*

4. Type the SNMP MIB-II sysContact value in the sysContact field.
5. Type the SNMP MIB-II sysName value in the sysName field.
6. Type the SNMP MIB-II sysLocation value in the sysLocation field.
7. Click OK to save the changes.

Important: You must download the SNMP MIB for your Dominion PX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see *Downloading SNMP MIB* (on page 139).

To configure SNMP managers:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click the Traps tab.
3. Select the Enabled checkbox in the "System Snmp Trap Event Rule" field.
4. Specify SNMP managers (destinations) by doing the following:
   a. You can specify up to 3 SNMP managers in the Host x fields, where x is a number between 1 and 3.
   b. Specify a port number for each SNMP manager in the Port x fields, where x is a number between 1 and 3.
   c. Specify a community string for each SNMP manager in the Community x fields, where x is a number between 1 and 3.
5. Click OK to save the changes.

Tip: The SNMP manager settings can be also set in the Event Rule Settings dialog. See **Modifying an Action** *(on page 109).*

Setting the Date and Time

You can set the internal clock on the Dominion PX device manually, or link to a Network Time Protocol (NTP) server and let it set the date and time for Dominion PX.

To set the date and time:

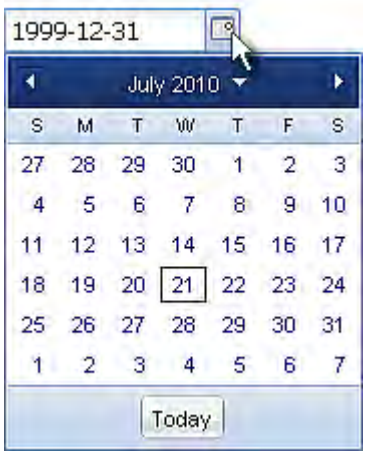
1. Choose Device Settings > Date/Time. The Configure Date/Time Settings dialog appears.
2. In the Time Zone field, click the drop-down arrow, and select your time zone from the list.
3. If the daylight saving time applies to your time zone, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.

   If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.
4. Choose one of the methods to set the date and time:
   - To customize the date and time, select the User Specified Time radio button, and then enter the date and time in appropriate fields. Use the yyyy-mm-dd format for the date and the hh:mm:ss format for the time.
     - To set the date, delete existing numbers in the Date field and type new ones, or click the calendar icon to select a date. See ***How to Use the Calendar*** (on page 61) for details.
     - The time is measured in 24-hour format so enter 13 for 1:00pm, 14 for 2:00pm, and so on. You can enter the time by deleting existing numbers and typing new ones in the hour, minute and second fields, or clicking the arrows to adjust each number.
   - To let an NTP server set the date and time, select the "Synchronize with NTP Server" radio button, and then enter the IP address or host name of the primary NTP server in the Primary Time Server field. A secondary NTP server is optional.

   Note: If the Dominion PX device's IP address is assigned through DHCP, the NTP server addresses may be automatically discovered. When this occurs, the data you entered in the fields of primary and secondary time server will be overridden.
5. Click OK to save the changes.

How to Use the Calendar

The calendar icon next to the Date field is a convenient tool to quickly change the year, month and date.



To select a date using the calendar:

1. To change the year shown in the calendar:
   a. Click , which is next to the year, and a list of years and months is displayed.

   b. Select the desired year from the list to the right and click OK. If the list does not show the desired year, click or to show additional years.
2. To change the month shown in the calendar, do either of the following:
   - Click or on the top of the calendar to switch between months.
   - Click to show a list of years and months. Select the desired month from the list to the left and click OK.

3. To select a date, do either of the following:
   - Click Today if you want to select today.

   Note: On the calendar, the date for today is marked with a red frame.

   - Click any date on the calendar.

Setting Data Logging

The data retrieval feature allows the retrieval of Dominion PX data by an SNMP manager, such as the data of PDU, line, and circuit breaker.

Dominion PX can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since Dominion PX's internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in log gets overwritten.

Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

Note: Dominion PX's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** *(on page 136) for more details. In addition, using an NTP time server ensures accurately time-stamped measurements.*

Enabling Data Logging

By default, data logging is disabled. Only users having the "Administrator" or "Change Data Logging Settings" permissions can enable or disable this feature. See ***Setting Up Roles*** (on page 68, on page 69).

To configure the data logging feature:

1. Choose Device Settings > Data Logging. The Data Logging Options dialog appears.
2. To enable the data logging feature, select the "enable" checkbox in the Enable Data Logging field.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Verify that all sensor logging is enabled. If not, click Enable All in Page to have all sensors selected.

5. Click OK to save the changes.

Note: Although it is possible to selectively enable/disable logging for individual sensors in Step 4, it is NOT recommended and this capability may be removed in the future.

Configuring the SMTP Settings

Dominion PX can be configured to send alerts or event messages to a specific administrator by email. To do this, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

Note: See **Configuring Event Rules** *(on page 102) for information on creating event rules to send email notifications.*

To set the SMTP server settings:

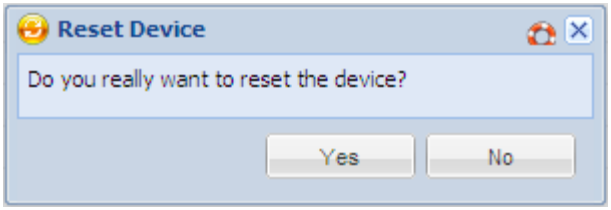
1. Choose Device Settings > SMTP Server. The SMTP Server Settings dialog appears.
2. Type the name or IP address of the mail server in the Server Name field.
3. Type the port number for the SMTP server in the Port field. The default is 25.
4. Type an email address for the sender in the Sender Email Address field.
5. Type the number of email retries in the Number of Sending Retries field. The default is 2 retries.
6. Type the time interval between email retries in the "Time Interval Between Sending Retries (in minutes)" field. The time is measured in minutes. The default is 2 minutes.
7. If your SMTP server requires password authentication, do this:
   a. Select the Server Requires Authentication checkbox.
   b. Type a user name in the User Name field.
   c. Type a password in the Password field.
8. Now that you have set the SMTP settings, you can test it to ensure it work properly. Do the following:
   a. Type the recipient's email address in the Recipient Email Address field.
   b. Click Send Test Email.
9. Click OK to save the changes.
10. Check if the recipient receives the email successfully.

Rebooting the Dominion PX Device

You can remotely reboot the Dominion PX device via the web interface.

To restart the device:

1. Choose Maintenance > Unit Reset. The Reset Device dialog appears.



2. Click Yes to reboot Dominion PX.
3. A message appears with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the reset is complete, the Login page opens. Now you can log back in to the Dominion PX device.

Note: If you are not redirected to the Login page after the reset is complete, click the underlined text "this link" in the message.

User Management

Dominion PX is shipped with one built-in user profile: **admin**, which is used for initial login and configuration. This profile has full system and outlet permissions, and should be reserved for the system administrator. It cannot be deleted and its permissions are not user-configurable except for the SNMP v3 permission.

All users must have a user profile, which specifies a login name and password, and contains additional (optional) information about the user. Every user profile must have at least a role to determine the user's system and outlet permissions. See ***Setting Up Roles*** (on page 68, on page 69).

Tip: By default, multiple users can log in simultaneously using the same login name.

Creating a User Profile

Creating new users adds a new login to Dominion PX.

To create a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.

2. Click New. The Create New User dialog appears.
3. Type the information about the user in the corresponding fields. Note that User Name, Password and Confirm Password fields are required.

Field	Type this...
User Name	The name the user enters to log in to Dominion PX. ▪ The name can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are NOT permitted
Full Name	The user's first and last names.
Password, Confirm Password	The password the user enters to log in. Type it first in the Password field and then again in the Confirm Password field. ▪ The password can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are permitted.
Telephone Number	A phone number where the user can be reached.
eMail Address	An email address where the user can be reached. ▪ The email can be up to 32 characters long. ▪ It is case sensitive.

4. Select the Enabled checkbox. If not, the user CANNOT log in to the Dominion PX device.
5. Select the "Force password change on next login" checkbox if you prefer a password change by the user when the user logs in for the first time after this checkbox is enabled.
6. Click the SNMPv3 tab to set the SNMPv3 access permission. The permission is disabled by default.
   a. To permit the SNMPv3 access by this user, select the "Enable SNMPv3 access" checkbox. Otherwise, leave the checkbox disabled.

Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See **Configuring the SNMP Settings** *(on page 58).*

---

   b. Set up SNMPv3 parameters if enabling the SNMPv3 access permission.

Field	Description
Security Level	Click the drop-down arrow to select a preferred

Field	Description
	security level from the list: ▪ NoAuthNoPriv: No authentication and no privacy. ▪ AuthNoPriv: Authentication and no privacy. ▪ AuthPriv: Authentication and privacy. This is the default.
Use Password as Authentication Pass Phrase	*This checkbox is configurable only if AuthNoPriv or AuthPriv is selected.* When the checkbox is selected, the authentication pass phrase is identical to the user's password. To specify a different authentication pass phrase, disable the checkbox.
Authentication Pass Phrase	Type the authentication pass phrase in this field if the "Use Password as Authentication Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Authentication Pass Phrase	Re-type the same authentication pass phrase for confirmation.
Use Authentication Pass Phrase as Privacy Pass Phrase	*This checkbox is configurable only if AuthPriv is selected.* When the checkbox is selected, the privacy pass phrase is identical to the authentication pass phrase. To specify a different privacy pass phrase, disable the checkbox.
Privacy Pass Phrase	Type the privacy pass phrase in this field if the "Use Authentication Pass Phrase as Privacy Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Privacy Pass Phrase	Re-type the same privacy pass phrase for confirmation.
Authentication Protocol	Click the drop-down arrow and select the desired authentication protocol from the list. Two protocols are available: ▪ MD5 ▪ SHA-1 (default)

Field	Description
Privacy Protocol	Click the drop-down arrow and select the desired privacy protocol from the list. Two protocols are available: ▪ DES (default) ▪ AES-128

7. Click the Roles tab to determine the permissions of the user.
8. Select one or multiple roles by selecting corresponding checkboxes.
   - The Admin role provides full permissions.
   - The Operator role provides limited permissions for frequently-used functions. See ***Setting Up Roles*** (on page 68, on page 69) for the scope of permissions. This role is selected by default.
   - If no roles meet your needs, you can:
     - *Modify the permissions of an existing role:* To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 70).
     - *Create a new role:* See ***Creating a Role*** (on page 69).

   Note: With multiple roles selected, a user has the union of all roles' permissions.
9. By default the temperature unit "Celsius" (°C) is applied to all temperatures shown on the Dominion PX web interface. To show the temperatures in Fahrenheit for this new user, click the Preferences tab, and select °F from the Temperature Unit's drop-down list.
10. Click OK to save the changes.

Modifying a User Profile

You can change any user profile's information except for the user name.

To modify a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. Make all necessary changes to the information shown.

   To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password is not changed.

5. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 64).
6. To change the permissions, click the Roles tab and do one of these:
   - Select or deselect any role's checkbox.
   - To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 70).
7. To change the temperature unit, click the Preferences tab, and select a different option from the Temperature Unit's drop-down list.
8. Click OK to save the changes.

Deleting a User Profile

Delete outdated or redundant user profiles when necessary.

To delete user profiles:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Changing the User List View

You may change the number of displayed columns or re-sort the list for better viewing the data. See ***Changing the View of a List*** (on page 48).

Setting Up Roles

A role defines the operations and functions a user is permitted to perform or access. Every user must be assigned at least a role.

Dominion PX is shipped with two built-in roles: **Admin** and **Operator**.

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:

  - View Event Settings

  - View Local Event Log

- Change Event Settings
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
- Change Own Password
- Switch Outlet (all outlets)

The Operator role is assigned to a newly created user profile by default. See ***Creating a User Profile*** (on page 64).

Setting Up Roles

A role defines the operations and functions a user is permitted to perform or access. Every user must be assigned at least a role.

Dominion PX is shipped with two built-in roles: **Admin** and **Operator**.

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:

  - View Event Settings
  - View Local Event Log
  - Change Event Settings
  - Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
  - Change Own Password

  The Operator role is assigned to a newly created user profile by default. See ***Creating a User Profile*** (on page 64).

Creating a Role

Create a new role when you need a new combination of permissions.

To create a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type the role's name in the Role Name field.
4. Type a description for the role in the Description field.
5. Click the Privileges tab to assign one or multiple permissions.
   a. Click Add. The "Add Privileges to new Role" dialog appears.

b. Select the permission you want from the Privileges list.

c. If the permission you selected contains any argument setting, the Arguments list is shown to the right. Then select one or multiple arguments.

d. Click Add to add the selected permission (and arguments if any).

e. Repeat Steps *a* to *d* until you add all necessary permissions.

6. Click OK to save the changes.

Now you can assign the new role to any users. See ***Creating a User Profile*** (on page 64) or ***Modifying a User Profile*** (on page 67).

Modifying a Role

You can change an existing role's settings except for the name.

To modify a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to modify by clicking it.
3. Click Edit or double-click the role. The Edit Role 'XXX' dialog appears, where XXX is the role name.

Tip: You can also access the Edit Role 'XXX' dialog by clicking the Edit Role button in the Edit User 'XXX' dialog.

4. Modify the text shown in the Description field if necessary.
5. To change the permissions, click the Privileges tab.

Note: You cannot change the Admin role's permissions.

6. To delete any permissions, do this:

a. Select the permission you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

b. Click Delete.

7. To add any permissions, do this:

a. Click Add. The Add Privileges to Role 'XXX' dialog appears, where XXX is the role name.

b. Select the permission you want from the Privileges list.

c. If the permission you selected contains any argument setting, the Arguments list is shown to the right. Then select one or multiple arguments.

d. Click Add to add the selected permission (and arguments if any).

e. Repeat Steps *a* to *d* until you add all necessary permissions.

8. To change a specific permission's arguments, do this:

a. Select the permission by clicking it.

b. Click Edit. The "Edit arguments of privilege 'XXX'" dialog appears, where XXX is the privilege name.

Note: If the permission you selected does not contain any arguments, the Edit button is disabled.

c. Select the argument you want. You can make multiple selections.

d. Click OK.

9. Click OK to save the changes.

Deleting a Role

You can delete any role other than the Admin role.

To delete a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Changing the Role List View

You may change the number of displayed columns or re-sort the list for better viewing the data. See ***Changing the View of a List*** (on page 48).

Access Security Control

Dominion PX provides tools to control access. You can require HTTPS encryption, enable the internal firewall and create firewall rules, and create login limitations.

Tip: You can also create and install the certificate or set up external authentication servers to control any access. See **Setting Up an SSL Certificate** *(on page 83) and* **Setting Up LDAP Authentication** *(on page 88).*

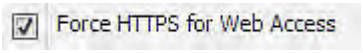
Forcing HTTPS Encryption

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the Dominion PX device so it is a more secure protocol than HTTP.

You can force users to access the Dominion PX web interface through the HTTPS protocol only. By default, this protocol is enabled.

To force HTTPS access to the web interface:

1. Choose Device Settings > Security > Force HTTPS for Web Access.
2. A message appears, prompting you to confirm the operation. Click Yes to enforce the HTTPS service.
3. Choose Device Settings > Security to verify the "Force HTTPS for Web Access" checkbox is selected as shown in this diagram.



If the checkbox is not selected, repeat these steps.

After enabling the HTTPS protocol, all access attempts using HTTP are redirected to HTTPS automatically.

Configuring the Firewall

Dominion PX has a firewall that you can configure to prevent specific IP addresses and ranges of IP addresses from accessing the Dominion PX device. By default the firewall is disabled.

To configure the firewall:

1. Enable the firewall. See ***Enabling the Firewall*** (on page 73).
2. Set the default policy. See ***Changing the Default Policy*** (on page 73).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See ***Creating Firewall Rules*** (on page 74).

Changes made to firewall rules take effect immediately. Any unauthorized IP activities cease instantly.

Note: The purpose of disabling the firewall by default is to prevent users from accidentally locking themselves out of the device.

Enabling the Firewall

The firewall rules, if any, take effect only after the firewall is enabled.

To enable the Dominion PX firewall:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Select the Enable IP Access Control checkbox. This enables the firewall.
3. Click OK to save the changes.

Changing the Default Policy

After enabling the firewall, the default policy is to accept traffic from all IP addresses. This means only IP addresses discarded by a specific rule will NOT be permitted to access Dominion PX.

You can change the default policy to Drop or Reject, in which case traffic from all IP addresses is discarded except the IP addresses accepted by a specific rule.

To change the default policy:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.
   - Accept: Accepts traffic from all IP addresses.
   - Drop: Discards traffic from all IP addresses, without sending any failure notification to the source host.
   - Reject: Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.
4. Click OK to save the changes. The new default policy is applied.

Creating Firewall Rules

Firewall rules determine whether to accept or discard traffic intended for Dominion PX, based on the IP address of the host sending the traffic. When creating firewall rules, keep these principles in mind:

- **Rule order is important.**

  When traffic reaches the Dominion PX device, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored by Dominion PX.

- **Subnet mask may be required.**

  When typing the IP address, you may or may not need to specify BOTH the address and a subnet mask. The default subnet mask is /32 (that is, 255.255.255.255). You must specify a subnet mask only when it is not the same as the default. For example, to specify a single address in a Class C network, use this format:

  x.x.x.x/24

  where */24* = a subnet mask of 255.255.255.0.

  To specify an entire subnet or range of addresses, change the subnet mask accordingly.

  Note: Valid IP addresses range from 0.0.0.0 through 255.255.255.255. Make sure the IP addresses entered are within the scope.

To create firewall rules:

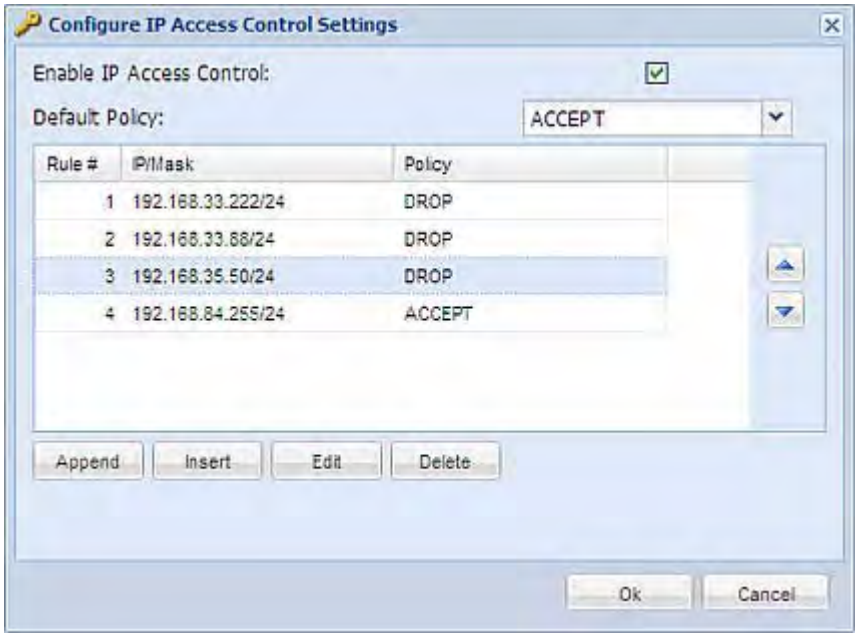
1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Create specific rules. See the table for different operations.

Action	Procedure

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type an IP address and subnet mask in the IP/Mask field.
	▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.
	  ▪ Accept: Accepts traffic from the specified IP address(es).
	  ▪ Drop: Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
	  ▪ Reject: Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

Action	Procedure
	▪ Click OK to save the changes. The system automatically numbers the rule.
Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert. The "Insert new Rule" dialog appears. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select Accept, Drop or Reject from the drop-down list in the Policy field. ▪ Accept: Accepts traffic from the specified IP address(es). ▪ Drop: Discards traffic from the specified IP address(es), without sending any failure notification to the source host. ▪ Reject: Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification. ▪ Click OK to save the changes. The system inserts the rule and automatically renumbers the following rules.

4. When finished, the rules appear in the Configure IP Access Control Settings dialog.



5. Click OK to save the changes. The rules are applied.

Editing Firewall Rules

When an existing firewall rule requires updates of IP address range and/or policy, modify them accordingly.

To modify a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Select the rule to be modified in the rules list.
4. Click Edit or double-click the rule. The Edit Rule dialog appears.
5. Make changes to the information shown.
6. Click OK to save the changes.
7. Click OK to quit the Configure IP Access Control Settings dialog, or the changes are lost.

Sorting Firewall Rules

The rule order determines which one of the rules matching the same IP address is performed.

To sort the firewall rules:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Select a specific rule by clicking it.
4. Click  or  to move the selected rule up or down until it reaches the desired location.
5. Click OK to save the changes.

Deleting Firewall Rules

When any firewall rules become obsolete or unnecessary, remove them from the rules list.

To delete a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Select the rule that you want to delete. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

4. Click Delete.
5. A message appears, prompting you to confirm the operation. Click Yes to remove the selected rule(s) from the rules list.
6. Click OK to save the changes.

Setting Up User Login Controls

You can set up login controls to make it more difficult for hackers to access Dominion PX and the devices connected to it. You can arrange to lock persons out after a specified number of failed logins, limit the number of persons who log in using the same user name at the same time, and force users to create strong passwords.

Enabling User Blocking

User blocking determines how many times a user can attempt to log in to Dominion PX and fail authentication before the user's login is blocked.

To enable user blocking:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the User Blocking section.
3. To enable the user blocking feature, select the "Block user on login failure" checkbox.
4. Type a number in the "Maximum number of failed logins" field. This is the maximum number of failed logins the user is permitted before the user's login is blocked from accessing the Dominion PX device.
5. To determine how long the login is blocked, select the desired length of time from the drop-down list in the "Block timeout" field. The following describes available options.
   - Infinite: This option sets no time limit on blocking the login.
   - X min: This type of option sets the time limit to X minutes, where X is a number.
   - X h: This type of option sets the time limit to X hours, where X is a number.
   - 1 d: This option sets the time limit to 1 day.
6. Click OK to save the changes.

Enabling Login Limitations

Login limitations determine whether more than one person can use the same login name at the same time, and how long users are permitted to stay idle before being forced to log out.

To enable login limitations:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the Login Limitations section.
3. To prevent more than one person from using the same login at the same time, select the "Prevent concurrent login with same username" checkbox.
4. To adjust how long users can remain idle before they are forcibly logged out by Dominion PX, select a time option in the Idle Timeout Period field. The default is 10 minutes.
   - X min: This type of option sets the time limit to X minutes, where X is a number.
   - X h: This type of option sets the time limit to X hours, where X is a number.
   - 1 d: This option sets the time limit to 1 day.
5. Click OK to save the changes.

Tip: Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to Dominion PX.

Enabling Strong Passwords

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the Dominion PX device. By default, strong passwords should be at least eight characters long and contain upper- and lower-case letters, numbers, and special characters, such as @ or &.

To force users to create strong passwords:

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Strong Passwords checkbox to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 32 characters

At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one special character	= Required
Number of restricted passwords in history	= 5

Note: The maximum password length accepted by Dominion PX is 32 characters.

3. Make necessary changes to the default settings.
4. Click OK to save the changes.

Enabling Password Aging

Password Aging determines whether users are required to change passwords at regular intervals. The default interval is 60 days.

To force users to change passwords regularly:

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Password Aging checkbox to enable the password aging feature.
3. To determine how often users are requested to change their passwords, select a number of days in the Password Aging Interval field. Users are required to change their password every time that number of days has passed.
4. Click OK to save the changes.

Setting Up Role Based Access Control Rules

Role based access control rules are similar to firewall rules, except they are applied to members sharing a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

To set up role based access control rules:

1. Enable the feature. See ***Enabling the Feature*** (on page 80).
2. Set the default policy. See ***Changing the Default Policy*** (on page 80).
3. Create rules specifying which addresses to accept and which ones to discard when the addresses are associated with a specific role. See ***Creating Role Based Access Control Rules*** (on page 80).

Changes made do not affect users currently logged in until the next login.

Enabling the Feature

You must enable this access control feature before any relevant rule can take effect.

To enable role based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Select the Enable Role Based Access Control checkbox. This enables the feature.
3. Click OK to save the changes.

Changing the Default Policy

The default policy is to accept all traffic from all IP addresses regardless of the role applied to the user.

To change the default policy:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Make sure the Enable Role Based Access Control checkbox is selected.
3. Select the action you want from the Default Policy drop-down list.
   - Allow: Accepts traffic from all IP addresses regardless of the user's role
   - Deny: Drops traffic from all IP addresses regardless of the user's role
4. Click OK to save the changes.

Creating Role Based Access Control Rules

Role based access control rules accept or drop traffic, based on the user's role and IP address. Like firewall rules, the order of rules is important, since the rules are executed in numerical order.

To create role based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Make sure the Enable Role Based Access Control checkbox is selected.
3. Create specific rules:

Action	Do this...

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type a starting IP address in the Starting IP Address field.
	▪ Type an ending IP address in the Ending IP Address field.
	▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only.
	▪ Select Allow or Deny from the drop-down list in the Policy field.
	  ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role
	  ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role
	▪ Click OK to save the changes.
	The system automatically numbers the rule.

Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
	▪ Click Insert. The "Insert new Rule" dialog appears.
	▪ Type a starting IP address in the Starting IP Address field.
	▪ Type an ending IP address in the Ending IP Address field.
	▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only.
	▪ Select Allow or Deny from the drop-down list in the Policy field.
	  ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role
	  ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role
	▪ Click OK to save the changes.
	The system inserts the rule and automatically renumbers the following rules.

4. Click OK to save the changes.

Editing Role Based Access Control Rules

You can modify existing rules when these rules do not meet your needs.

To modify a role based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Ensure the Enabled Role Based Access Control checkbox is selected.
3. Select the rule to be modified in the rules list.
4. Click Edit or double-click the rule. The Edit Rule dialog appears.
5. Make changes to the information shown.
6. Click OK to save the changes.

Sorting Role Based Access Control Rules

Similar to firewall rules, the order of role based access control rules determines which one of the rules matching the same IP address is performed.

To sort role based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Ensure the Enabled Role Based Access Control checkbox is selected.
3. Select a specific rule by clicking it.
4. Click  or  to move the selected rule up or down until it reaches the desired location.
5. Click OK to save the changes.

Deleting Role Based Access Control Rules

When any access control rule becomes unnecessary or obsolete, remove it.

To delete a role based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Ensure the Enabled Role Based Access Control checkbox is selected.
3. Select the rule to be deleted in the rules list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
4. Click Delete.

5. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
6. Click OK to save the changes.

Setting Up an SSL Certificate

Having an X.509 digital certificate ensures that both parties in an SSL connection are who they say they are.

To obtain a certificate for Dominion PX, create a Certificate Signing Request (CSR) and submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with an SSL certificate, which you must install on the Dominion PX device.

Note: See **Forcing HTTPS Encryption** *(on page 72) for instructions on forcing users to employ SSL when connecting to Dominion PX.*

A CSR is not required in either of the following scenarios:

- You decide to generate a *self-signed* certificate on the Dominion PX device.
- Appropriate, valid certificate and key files have been available.

Certificate Signing Request

When appropriate certificate and key files for Dominion PX are NOT available, one of the alternatives is to create a CSR and private key on the Dominion PX device, and send the CSR to a CA for signing the certificate.

Creating a Certificate Signing Request

Follow this procedure to create the CSR for your Dominion PX device.

To create a CSR:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.
   - In the Subject section:

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.

Field	Type this information
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your Dominion PX device.
Email Address	An email address where you or another administrative user can be reached.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields. If you generate a CSR without values entered in the required fields, you cannot obtain third party certificates.

- In the Key Creation Parameters section:

Field	Do this
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the Dominion PX device's response.
Self Sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**
Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional, and the value should be 4 to 64 characters long. The password is case sensitive, so ensure you capitalize the letters correctly.
Confirm Challenge	Type the same password again for confirmation.

4. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.
5. To download the newly-created CSR to your computer, click Download Certificate Signing Request.
   a. You are prompted to open or save the file. Click Save to save it on your computer.
   b. After the file is stored on your computer, submit it to a CA to obtain the digital certificate.
   c. If desired, click Delete Certificate Signing Request to remove the CSR file permanently from the Dominion PX device.
6. To store the newly-created private key on your computer, click Download Key. You are prompted to open or save the file. Click Save to save it on your computer.
7. Click Close to quit the dialog.

Installing a CA-Signed Certificate

After the CA provides a signed certificate according to the CSR you submitted, you must install it on the Dominion PX device.

To install the certificate:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. In the Certificate File field, click Browse to select the certificate file provided by the CA.
4. Click Upload. The certificate is installed on the Dominion PX device.

   Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

5. Click Close to quit the dialog.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the Dominion PX device are unavailable, the alternative other than submitting a CSR to the CA is to generate a self-signed certificate.

To create and install a self-signed certificate:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your Dominion PX device.
Email Address	An email address where you or another administrative user can be reached.

Field	Type this information
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the Dominion PX device's response.
Self Sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate is valid in this field.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear after the Self Sign checkbox is selected.

4. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.
5. You can also do any of the following:
   - Click "Install Key and Certificate" to immediately install the self-signed certificate and private key. When any confirmation and security messages appear, click Yes to continue.

   Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

   - To download the self-signed certificate or private key, click Download Certificate or Download Key. You are prompted to open or save the file. Click Save to save it on your computer.
   - To remove the self-signed certificate and private key permanently from the Dominion PX device, click "Delete Key and Certificate".
6. If you installed the self-signed certificate in Step 5, after the installation completes, the Dominion PX device resets and the login page re-opens.

Installing Existing Key and Certificate Files

If the SSL certificate and private key files are already available, you can install them directly without going through the process of creating a CSR or a self-signed certificate.

To install the existing key and certificate files:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.

3. Select the "Upload Key and Certificate" checkbox. The Key File and Certificate File fields appear.
4. In the Key File field, click Browse to select the private key file.
5. In the Certificate File field, click Browse to select the certificate file.
6. Click Upload. The selected files are installed on the Dominion PX device.

   Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

7. Click Close to quit the dialog.

Downloading Key and Certificate Files

You can download the key and certificate files currently installed on the Dominion PX device for backup or other operations. For example, you can install the files on a replacement Dominion PX device, add the certificate to your browser and so on.

To download the certificate and key files from a Dominion PX device:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. The Active SSL Certificate tab should open. If not, click it.
3. Click Download Key to download the private key file installed on the Dominion PX device. You are prompted to open or save the file. Click Save to save it on your computer.
4. Click Download Certificate to download the certificate file installed on the Dominion PX device. You are prompted to open or save the file. Click Save to save it on your computer.
5. Click Close to quit the dialog.

Setting Up LDAP Authentication

For security purposes, users attempting to log in to Dominion PX must be authenticated. Dominion PX supports the access using one of the following authentication mechanisms:

- Local database of user profiles on the Dominion PX device
- Lightweight Directory Access Protocol (LDAP)

By default, Dominion PX is configured for local authentication. If you stay with this method, you do not need to do anything other than create user profiles for each authorized user. If you prefer to use an external LDAP server, you must:

- Provide Dominion PX with information about the LDAP server.
- Create user profiles for users who are authenticated externally because a user profile on the Dominion PX device determines the role(s) applied to the user, and determines the permissions for the user accordingly.

When configured for LDAP authentication, all Dominion PX users must have an account on the LDAP server. Local-authentication-only users will have no access to Dominion PX except for the admin, who always can access Dominion PX.

Gathering the LDAP Information

It requires knowledge of your LDAP server and directory settings to configure Dominion PX for LDAP authentication. If you are not familiar with the settings, consult your LDAP administrator for help.

To configure LDAP authentication, you need to check:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over SSL) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*

  - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

Adding the LDAP Server Settings

To activate and use external LDAP/LDAPS server authentication, enable LDAP authentication and enter the information you have gathered for any LDAP/LDAPS server.

Note: An LDAPS server refers to an SSL-secured LDAP server.

To add the LDAP/LDAPS server settings:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate remote LDAP/LDAPS server authentication.
3. Click New to add an LDAP/LDAPS server for authentication. The "Create new LDAP Server Configuration" dialog appears.
4. IP Address / Hostname - Type the IP address or hostname of your LDAP/LDAPS authentication server.

   Important: Without the SSL encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the SSL encryption is enabled.
5. Type of external LDAP/LDAPS server. Choose from among the options available:
   - OpenLDAP
   - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
6. LDAP over SSL - Select this checkbox if you would like to use SSL. Secure Sockets Layer (SSL) is a cryptographic protocol that allows Dominion PX to communicate securely with the LDAP/LDAPS server. A certificate file is required when enabling the encryption.
7. Port - The default Port is 389. Either use the standard LDAP TCP port or specify another port.
8. SSL Port - The default is 636. Either use the default port or specify another port. This field is enabled when the "LDAP over SSL" checkbox is selected.

9. Use only trusted LDAP Server Certificates - Select this checkbox if you would like to use a trusted LDAP server certificate file, that is, a certificate file signed by the CA. When NOT selected, you can use all LDAP/LDAPS server certificates, including a self-signed certificate file.
10. Server Certificate - Consult your authentication server administrator to get the CA certificate file for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. This field is required when the "LDAP over SSL" checkbox is selected.
11. Anonymous Bind - If the external **OpenLDAP** server permits anonymous queries to the LDAP directory, you may select this checkbox. When selected, go to Step 15 since it is not necessary to specify the Bind Distinguished Name (DN) and Bind Password.
12. Use Bind Credentials - To provide authentication information for the "bind" operation to the **Microsoft Active Directory** server, select this checkbox.
13. Bind DN - Specify the DN of the user who is permitted to search the LDAP directory in the defined search base.
14. Bind Password and Confirm Bind Password - Enter the Bind password in the Bind Password field first and then the Confirm Bind Password field. This information is required if the Use Bind Credentials checkbox is selected.
15. Base DN for Search - Enter the name you want to bind against the LDAP/LDAPS (up to 31 characters), and where in the database to begin searching for the specified Base DN. An example Base Search value might be: `cn=Users,dc=raritan,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.
16. Type the following information in the corresponding fields. LDAP needs this information to verify user names and passwords.
    - Login name attribute (also called AuthorizationString)
    - User entry object class
    - User search subfilter (also called BaseSearch)

    Note: Dominion PX will preoccupy the login name attribute and user entry object class with default values, which should not be changed unless required.
17. Active Directory Domain - Type the name of the Active Directory Domain. For example, testradius.com. Consult with your Active Directory Administrator for a specific domain name.
18. To verify if the LDAP/LDAPS configuration is done correctly, you may click Test Connection to check whether Dominion PX can connect to the LDAP/LDAPS server successfully.

Tip: You can also do this by using the Test Connection button in the Authentication Settings dialog.

19. Click OK to save the changes. The new LDAP server is listed in the Authentication Settings dialog.
20. To add additional LDAP/LDAPS servers, repeat Steps 3 to 19.
21. Click OK to save the changes. The LDAP authentication is now in place.

Note: If the Dominion PX clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure Dominion PX and the LDAP server to use the same NTP server.

More Information about AD Configuration

For more information about the LDAP configuration using Microsoft Active Directory, see ***LDAP Configuration Illustration*** (on page 229).

Sorting the LDAP Access Order

The order of the LDAP list determines the access priority of remote LDAP/LDAPS servers. Dominion PX first tries to access the top LDAP/LDAPS server in the list for authentication, then the next one if the access to the first one fails, and so on until the Dominion PX device successfully connects to one of the listed LDAP/LDAPS servers.

Note: After successfully connecting to one LDAP/LDAPS server, Dominion PX STOPS trying to access the remaining LDAP/LDAPS servers in the list regardless of the user authentication result.

To re-sort the LDAP server access list:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server whose priority you want to change.
3. Click "Move up" or "Move down" until the selected server reaches the desired position in the list.
4. Click OK to save the changes.

Testing the LDAP Server Connection

You can test the connection to any LDAP/LDAPS server to verify the server accessibility or the validity of the authentication settings.

To test the connection to an LDAP/LDAPS server:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to test.
3. Click Test Connection to start the connection test.

Editing the LDAP Server Settings

If the configuration on any LDAP/LDAPS server has been changed, such as the port number, bind DN and password, you must modify the LDAP/LDAPS settings on the Dominion PX device accordingly, or the authentication fails.

To modify the LDAP authentication configuration:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to edit.
3. Click Edit. The Edit LDAP Server Configuration dialog appears.
4. Make necessary changes to the information shown.
5. Click OK to save the changes.

Deleting the LDAP Server Settings

You can delete the authentication settings of a specific LDAP/LDAPS server when the server is not available or used for remote authentication.

To remove one or multiple LDAP/LDAPS servers:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click OK to save the changes.

Disabling the LDAP Authentication

When the remote authentication service is disabled, Dominion PX authenticates users against the local database stored on the Dominion PX device.

To disable the LDAP authentication service:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Local Authentication radio button.
3. Click OK to save the changes.

Enabling LDAP and Local Authentication Services

To make authentication function properly all the time -- even when external authentication is not available, you can enable both the local and remote authentication services.

When both authentication services are enabled, Dominion PX follows these rules for authentication:

- When any of the LDAP/LDAPS servers in the access list is accessible, Dominion PX authenticates against the connected LDAP/LDAPS server only.
- When the connection to every LDAP/LDAPS server fails, Dominion PX allows authentication against the local database.

To enable both authentication services:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Ensure the LDAP radio button has been selected.
3. Select the "Use Local Authentication if Remote Authentication service is not available" checkbox.
4. Click OK to save the changes.

Outlet Management

Dominion PX allows you to remotely customize the name of each outlet through the web interface. In addition, you can remotely check which circuit breaker is associated with each outlet.

Naming Outlets

You can give each outlet a name up to 32 characters long to identify the equipment connected to it.

The customized name is displayed along with the label in parentheses throughout the web interface.

Note: In this context, the label refers to the outlet number.

To name an outlet:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click Outlets in the Dominion PX Explorer pane, and the Outlets page opens in the right pane.
3. Click the outlet you want in the right pane.
4. Click Setup. The setup dialog for the selected outlet appears.
5. Type a name in the Outlet Name field.
6. Click OK to save the changes.

Checking Associated Circuit Breakers

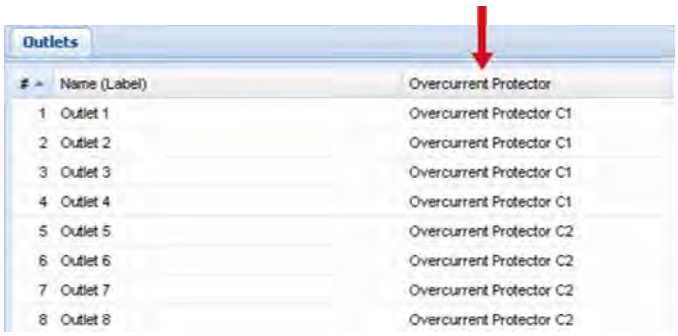
To find out each outlet is protected by which circuit breaker, you can check the Outlets page.

Tip: This type of information is also available by choosing Maintenance > Device Information. See **Displaying the PDU Information** *(on page 52).*

To check associated circuit breaker for all outlets:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click Outlets in the Dominion PX Explorer pane, and the Outlets page opens in the right pane.

All outlets are listed with associated circuit breakers shown in the Overcurrent Protector column.



Inlet and Circuit Breaker Management

You can name each inlet and circuit breaker or monitor their status.

Naming the Inlet

You can customize the inlet's name for your own purpose.

The customized name is displayed along with the label in parentheses throughout the web interface.

Note: In this context, the label refers to the inlet number, such as I1.

To name the inlet:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click Inlet I1 in the Dominion PX Explorer pane, and the Inlet I1 page opens in the right pane.
3. Click Setup. The Inlet Setup dialog appears.
4. Type a new name in the Name field.
5. Click OK to save the changes.

Naming Circuit Breakers

You can name each circuit breaker for easily identifying them.

The customized name is displayed along with the label in parentheses throughout the web interface.

Note: In this context, the label refers to the circuit breaker number, such as C1.

To name a circuit breaker:

1. Expand the Overcurrent Protectors folder to show all circuit breakers in the Dominion PX Explorer pane. See ***Expanding the Tree*** (on page 43).
2. Click the desired circuit breaker in the Dominion PX Explorer pane, and the page for this circuit breaker opens in the right pane.
3. Click Setup. The Overcurrent Protector Setup dialog appears.
4. Type a new name in the Name field.
5. Click OK to save the changes.

Monitoring the Inlet

You can view the inlet's details, including its:

- Label (number)
- Customized name
- Inlet sensor readings:
  - Active energy (Wh)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - RMS current per line (A)
  - RMS voltage per line pair (V)

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or the circuit breaker has tripped. See **The Yellow- or Red-Highlighted Reading** *(on page 47).*

There are two ways to access the inlet information.

To get the overview of the inlet status:

1. Click the Dashboard icon in the Dominion PX Explorer pane, and the Dashboard page opens in the right pane.

2. Locate the Inlet section on the Dashboard page.

To view the inlet's details:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click Inlet I1 in the Dominion PX Explorer pane, and the Inlet I1 page opens in the right pane.

Note: A few Dominion PX models may show some current being drawn or power consumption while no loads are physically attached to the PDU. For details, see **Non-Zero Readings While No Loads Attached** *(on page 240).*

Monitoring Circuit Breakers

Each circuit breaker on the Dominion PX device delivers power to a bank of outlets, and draws power from one or two lines.

You can view the circuit breaker's details, including its:

- Label (number)
- Name
- Status (closed/open)
- Lines associated with the circuit breaker
- Sensor readings:

  - Current drawn (A)

  - Current remaining (A)

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or the circuit breaker has tripped. See **The Yellow- or Red-Highlighted Reading** *(on page 47).*

You can view the summary of all circuit breakers at a time or the status of individual circuit breakers.

To view all circuit breakers' status:

You can check the status of all circuit breakers at a time via either the Dashboard or Overcurrent Protectors page.

- **Using the Dashboard page:**

a. Click the Dashboard icon in the Dominion PX Explorer pane, and the Dashboard page opens in the right pane.

b. Locate the Overcurrent Protectors section on the Dashboard page.

- **Using the Overcurrent Protectors page:**

a. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).

b. Click Overcurrent Protectors in the Dominion PX Explorer pane, and the Overcurrent Protectors page opens in the right pane.

To view a circuit breaker's details:

1. Expand the Overcurrent Protectors folder to show all circuit breakers in the Dominion PX Explorer pane. See ***Expanding the Tree*** (on page 43).
2. Click the desired circuit breaker in the Dominion PX Explorer pane, and the page for this circuit breaker opens in the right pane.

Setting Power Thresholds

Setting and enabling the thresholds causes Dominion PX to generate alert notifications when it detects that any component's power state crosses the thresholds.

Usually there are four thresholds for each sensor: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

- Upper and Lower Warning thresholds indicate the sensor reading enters the warning range before the critical threshold.
- Upper and Lower Critical thresholds indicate the sensor reading is at the critical level.

To avoid generating a large amount of alert events, the deassertion hysteresis for each threshold is enabled. You can change the default hysteresis value if necessary. For more information on the deassertion hysteresis, see ***What is Deassertion Hysteresis?*** (on page 100) .

Note: After setting the thresholds, remember to configure the event rules. See **Configuring Event Rules** *(on page 102).*

Setting Inlet Thresholds

You can set the inlet thresholds so that the alerts are generated when the inlet current and/or voltage crosses the thresholds.

To set the inlet thresholds:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click Inlet I1 in the Dominion PX Explorer pane, and the Inlet I1 page opens in the right pane.
3. Click Setup. The Inlet Setup dialog appears.

4. In the Threshold Configuration table, click the sensor row that you want to configure.
5. Click Edit. A threshold setup dialog for the selected sensor appears.
6. Set up the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 100) for the function of deassertion hysteresis.
   - To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. This value determines how many samples should be generated before any warning or critical condition is asserted. See ***What is Assertion Timeout?*** (on page 101).
7. Click Ok in the threshold setup dialog to retain the changes.
8. To set the thresholds for other sensors, repeat Steps 4 to 8.
9. Click OK to save the changes.

Important: The final step is required or the threshold changes are not saved.

Setting Circuit Breaker Thresholds

Setting the circuit breaker thresholds enables the PDU to generate alerts when the circuit breaker crosses the thresholds.

To set the circuit breaker thresholds:

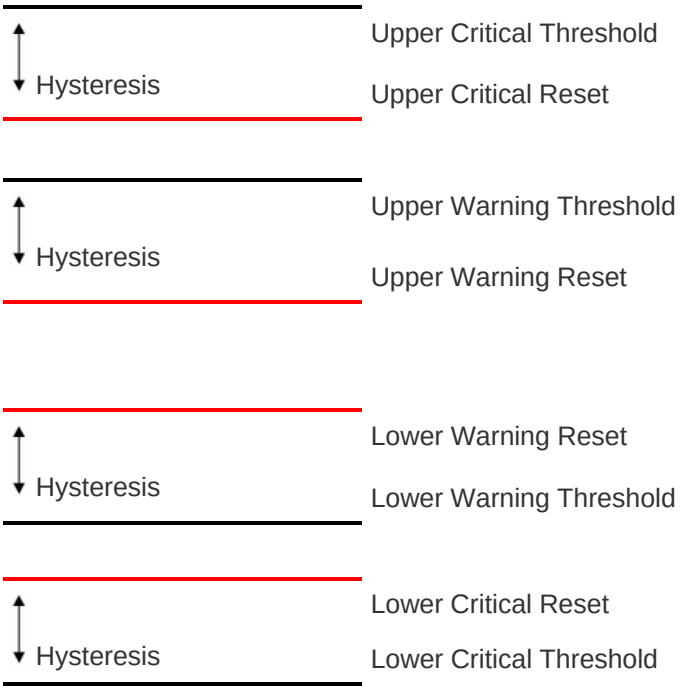
1. Expand the Overcurrent Protectors folder to show all circuit breakers in the Dominion PX Explorer pane. See ***Expanding the Tree*** (on page 43).
2. Click the desired circuit breaker in the Dominion PX Explorer pane, and the page for this circuit breaker opens in the right pane.
3. Click Setup. The Overcurrent Protector Setup dialog appears.
4. In the Threshold Configuration table, click the sensor row that you want to configure.
5. Click Edit. A threshold setup dialog for the selected sensor appears.
6. Set up the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.

- To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
- After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
- To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 100) for the function of deassertion hysteresis.
- To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. This value determines how many samples should be generated before any warning or critical condition is asserted. See ***What is Assertion Timeout?*** (on page 101).

7. Click OK to save the changes.

What is Deassertion Hysteresis?

The hysteresis setting determines when a threshold condition is reset. This diagram illustrates how hysteresis values relate to thresholds:



The hysteresis values define a reset threshold. For upper thresholds, the measurement must fall past this reset threshold before a deassertion event is generated. For lower thresholds, the measurement must rise above this reset threshold before a deassertion event is generated.

Example: When Hysteresis is Useful

This example demonstrates when a deassertion hysteresis is useful.

The current critical threshold for the inlet is set to 19 amps (A). The current draw rises to 20A, triggering a Current Critical alert. The current then continues to fluctuate between 18.1A and 20A.

With the hysteresis set to 1A, Dominion PX continues to indicate that the current on the inlet is above critical. Without hysteresis (that is, the hysteresis is set to zero), Dominion PX would de-assert the condition each time the current dropped to 18.9A, and re-assert the condition each time the current reached 19A or higher. With the fluctuating current, this could result in a number of repeating SNMP traps, and/or an e-mail account full of repeating SMTP alert notifications.

Example: When to Disable Hysteresis

This is an example of when you want to disable hysteresis for the inlet -- that is, set the hysteresis to zero.

The upper warning threshold for current in the inlet is set to 15A. In normal usage, the inlet draws 14.6A of current. A spike in demand causes the current to reach 16A, triggering an alert. The current then settles to the normal draw of 14.6A.

With hysteresis set to zero, Dominion PX de-asserts the condition once the current drops to 14.9A. Otherwise the inlet would still be considered above the warning threshold as long as the current never dropped to 14.0A. The condition would not de-assert, even if the current returned to normal.

What is Assertion Timeout?

When the assertion timeout is enabled, a specific number of consecutive measurement samples that crosses a specific threshold must be generated before any warning or critical condition is asserted. This prevents a number of threshold alerts from being generated if the measurements return to normal immediately after rising above any upper threshold or dropping below any lower threshold.

Configuring Event Rules

A benefit of the product's intelligence is its ability to notify you of and react to a change in conditions. This event notification or reaction is an "event rule."

Dominion PX is shipped with two built-in event rules, which cannot be deleted.

- System Event Log Rule: This rule causes ANY event occurred to Dominion PX to be recorded in the internal log. The rule is enabled by default.
- System SNMP Trap Rule: This rule causes SNMP traps to be sent to specified IP addresses or hosts when ANY event occurs to Dominion PX. The rule is disabled by default.

If these two do not satisfy your needs, you can create additional rules to respond to different events.

Note: Internet Explorer® 8 (IE8) does not use compiled JAVA script. When using IE8 to create or change event rules, the CPU performance may be degraded, resulting in the appearance of the connection time out message. When this occurs, click Ignore to continue.

Components of an Event Rule

An event rule defines what Dominion PX does in certain situations and is composed of two parts:

- Event: This is the situation where Dominion PX or part of it meets a certain condition. For example, the inlet's voltage exceeds the warning threshold.
- Action: This is the response to the event. For example, Dominion PX notifies the system administrator of the event and records the event in the log.

Creating an Event Rule

The best way to create a new set of event rule, in sequence, is:

- Create actions for responding to one or multiple events.
- Create rules to determine what actions are taken when these events occur.

Creating Actions

Dominion PX comes with two built-in actions:

- System Event Log Action: This action records the selected event in the internal log when the event occurs.
- System SNMP Trap Action: This action sends SNMP traps to one or multiple IP addresses after the selected event occurs.

Note: No IP addresses are specified for the "System SNMP Trap Action" by default so you must specify IP addresses before applying this action to any event rule.

The built-in actions cannot be deleted. If these actions do not satisfy your needs, then create new ones.

To create new actions:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New Action.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number.
5. In the Action field, click the drop-down arrow, and select the desired action from the list in response to the selected event.
   - Log event message: This option records the selected events in the internal log.
   - Send SMTP message: This option notifies one or multiple persons of the selected events by e-mail.
   - Send SNMP trap: This option sends SNMP traps to one or multiple SNMP managers.
   - Syslog message: This option makes Dominion PX automatically forward event messages to the specified syslog server.
6. Complete further settings for the selected action if necesssary.
   - Send SMTP message: This option requires you to specify the email address(es) of the recipient(s), and determine which SMTP server settings to apply.

- In the "Recipients email addresses" field, specify the email address(es). Use a comma to separate multiple email addresses.
- To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox. To use a different SMTP server, select the Use Custom SMTP Settings checkbox. If the SMTP server settings are not configured yet, click Configure. See ***Configuring the SMTP Settings*** (on page 63) for the information of each field.

- Send SNMP trap: You need to specify SNMP managers and associated settings for this option.
  - You can specify up to 3 SNMP managers in the Host x fields, where x is a number between 1 and 3.
  - Specify a port number for each SNMP manager in the Port x fields, where x is a number between 1 and 3.
  - Specify a community string for each SNMP manager in the Community x fields, where x is a number between 1 and 3.
- Syslog message: Specify the IP address to which syslog is forwarded in the "Syslog server" field, and an appropriate port number in the Port field.

7. Click Save to save the new action.

Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.

8. To create additional actions, repeat Steps 3 to 7.
9. Click Close to quit the dialog.

Creating Rules

After required actions are available, you can create event rules to determine what actions are taken to respond to specific events.

By default, Dominion PX provides two built-in event rules -- System Event Log Rule and System SNMP Trap Rule. If the built-in rules do not satisfy you needs, create new ones.

Note: For information on the built-in event rules, see **Configuring Event Rules** *(on page 102).*

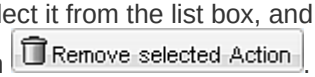
To create event rules:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.

2. On the Rules tab, click New Rule.
3. In the "Rule name" field, type a new name for identifying the rule. The default name is New Rule <number>, where <number> is a sequential number.
4. Select the Enabled checkbox to enable this event rule.
5. Click Event to select an event for which you want to trigger an action. A pull-down menu showing all types of events appears.
   - Select the desired event type from the pull-down menu, and if a submenu appears, continue the navigation until the desired event is selected.

   Note: Selection of the option "<Any sub-event>" means that all events occurred to the selected menu item will trigger actions.
6. In the "Trigger condition" field, select the "Asserted," "Deasserted" or "Both" radio button.
   - Asserted: Dominion PX takes the action only when the event occurs. This means the status of the described event transits from FALSE to TRUE.
   - Deasserted: Dominion PX takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE.
   - Both: Dominion PX takes the action both when the event occurs (asserts) and when the event condition disappears (deasserts).
7. In the Actions field, click the drop-down arrow, select the desired action from the list, and click the Add Action button 

to add the action.

   The added action will be listed in the list box to the right of the Actions filed.
8. To add additional actions, repeat Step 7.
9. To remove any added action, select it from the list box, and click the "Remove selected Action" button 

.
10. Click Save to save the new event rule.

    Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.
11. Repeat Steps 2 to 10 to create additional event rules.
12. Click Close to quit the dialog.

Sample Event Rules

Sample PDU-Level Event Rule

In this example, we want Dominion PX to record the firmware upgrade failure in the internal log when it happens. The sample event rule looks like this:

- Event: Events > Device > Firmware update failed
- Trigger condition: asserted
- Actions: System Event Log Action

To create the above event rule:

1. Select Events > Device to indicate we are specifying an event at the PDU level.
2. Select "Firmware update failed" in the submenu because we want Dominion PX to respond to the event related to firmware upgrade failure.
3. Select System Event Log Action as we intend to record the firmware update failure event in the internal log.
4. Select the "asserted" radio button since we want the selected event to be recorded only when it occurs.

Sample Outlet-Level Event Rule

In this example, we want Dominion PX to send SNMP traps to the SNMP manager both when any sensor reading of outlet 3 crosses any threshold and when it returns to normal. To do that we would set up an event rule like this:

- Event: Events > Outlet > Outlet 3 > Sensor > Any sub-event
- Trigger condition: both
- Actions: System SNMP Trap Action

To create the above event rule:

1. Select Events > Outlet to indicate we are specifying an event at the outlet level.
2. Select "Outlet 3" from the submenu because that is the outlet in question.
3. Select "Sensor" to refer to sensor readings.
4. Select "Any sub-event" because we want to specify all events related to all types of outlet sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.

5. Select "System SNMP Trap Action" to send SNMP traps to respond to the specified event.
6. Select the "both" radio button so that the SNMP traps are sent both when any sensor reading of outlet 3 moves past any threshold into the warning or critical range and when the sensor reading returns to normal.

   For example, when the outlet 3's voltage crosses into the upper warning range, the SNMP traps are sent, and when the voltage drops below the upper warning threshold, the SNMP traps are sent again.

Sample Inlet-Level Event Rule

In this example, we want Dominion PX to send SNMP traps to the SNMP manager both when any sensor reading of the Inlet I1 crosses any threshold and when it returns to normal. The event rule is set like this:

- Event: Events > Inlet > Inlet I1 > Sensor > Any sub-event
- Trigger condition: both
- Actions: System SNMP Trap Action

To create the above event rule:

1. Select Events > Inlet to indicate we are specifying an event at the inlet level.
2. Select "Inlet I1" from the submenu because that is the inlet in question.
3. Select "Sensor" to refer to sensor readings.
4. Select "Any sub-event" because we want to specify all events related to all types of inlet sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. Select "System SNMP Trap Action" to send SNMP traps to respond to the specified event.
6. Select the "both" radio button so that the SNMP traps are sent both when any sensor reading of Inlet I1 moves past any threshold into the warning or critical range and when the sensor reading returns to normal.

   For example, when the Inlet I1's voltage crosses into the upper warning range, the SNMP traps are sent, and when the voltage drops below the upper warning threshold, the SNMP traps are sent again.

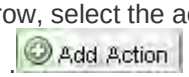
Modifying an Event Rule

You can change an event rule's event, action, trigger condition and other settings, if any.

Exception: Events and actions selected in the built-in event rules are not changeable, including System Event Log Rule and System SNMP Trap Rule.

To modify an event rule:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the event rule that you want to modify in the left pane.
3. To disable the event rule, deselect the Enabled checkbox.
4. To change the event, click the desired tab in the Event field and select a different item from the pull-down menu or submenu.

   For example, in a user activity event rule for the "admin" user, you can click the "admin" tab to display a pull-down submenu showing all user names, and then select a different user name or all user names (referred to as <*Any user*>).
5. If radio buttons are available, you may select a radio button other than the current selection to change the rule triggering condition.
6. To change the action(s), do any of the following in the Actions field:
   - To add a new action, click the drop-down arrow, select the action from the list, and click the Add Action button . 
   - To remove any added action, select it from the list box, and click the "Remove selected Action" button  .
7. Click Save to save the changes.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.
8. Click Close to quit the dialog.

Modifying an Action

An existing action can be changed so that all event rules where this action is involved change their behavior accordingly.

Exception: The built-in action "System Event Log Action" is not user-configurable.

To modify an action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Select the action that you want to modify from the left list.
4. Make necessary changes to the information shown.
5. Click Save to save the changes.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.

6. Click Close to quit the dialog.

Deleting an Event Rule or Action

If any event rule or action is obsolete, simply remove it.

Note: You cannot delete the built-in event rules and actions.

To delete an event rule or action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. To delete an event rule:
   a. Ensure the Rules tab is selected. If not, click the Rules tab.
   b. Select the desired rule from the left list, and click Delete Rule.
   c. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
3. To delete an action:
   a. Click the Actions tab.
   b. Select the desired action from the left list, and click Delete Action.
   c. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
4. Click Close to quit the dialog.

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing Dominion PX to generate an alert. The measurement then returns to a value within the threshold, but Dominion PX does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking Dominion PX uses. See ***What is Deassertion Hysteresis?*** (on page 100).

Managing Event Logging

By default, Dominion PX captures certain system events and saves them in a local (internal) event log.

Viewing the Local Event Log

You can view up to 2,000 historical events that occurred to the Dominion PX device in the local event log.

When the log already contains 2,000 entries, each new entry overwrites the oldest entry.

To display the local log:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.

   Each event entry in the local log consists of:

   - Date and time of the event
   - Type of the event
   - A description of the event

2. The dialog shows the last page by default. You can:

   - Switch between different pages by doing one of the following:

     - Click  or  to go to the first or last page.

     - Click  or  to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.

   - Select a log entry from the list and click Show Details to view detailed information of the selected entry.

   Note: Sometimes when the dialog is too narrow, the icon » takes the place of the Show Details button. In that case, click » to view details.

3. Enlarge the dialog if necessary. See ***Resizing a Dialog*** (on page 49).

4. You can re-sort the list or change the columns displayed. See ***Changing the View of a List*** (on page 48).
5. Click Close to quit the dialog.

Clearing Event Entries

If it is not necessary to keep existing event history, you can remove all of it from the local log.

To delete all event entries:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.
2. Click Clear Event Log.
3. Click Close to quit the dialog.

Viewing Connected Users

You can see which users are being connected to the Dominion PX device and their status on the web interface. Besides, if you have the administrator privileges, you can terminate any user's connection to the Dominion PX device.

To view connected users:

1. Choose Maintenance > Connected Users. The Connected Users dialog appears, showing a list of connected users with the following information:
   - User Name -- the login name of each connected user.
   - IP Address -- the IP address of each user's host.
   - Client Type -- the column shows the interface through which the user is connected to Dominion PX.
   - Idle Time -- the length of time for which a user remains idle. The unit "min" represents minutes.
2. To disconnect any user, click the corresponding Disconnect button.
   - A dialog appears, prompting you to confirm the operation.
   - Click Yes to disconnect the user or No to abort the operation.
3. You may change the sorting order of the list if necessary. See ***Changing the Sorting*** (on page 49).
4. Click Close to quit the dialog.

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the Dominion PX device continuously ping them. An IT device's successful response to the pings indicates that the IT device is still alive and can be remotely accessed.

Adding IT Devices for Ping Monitoring

You can have Dominion PX monitor the accessibility of any IT equipment, such as DB servers and remote authentication servers.

To add IT equipment for ping monitoring:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New. The Add New Server dialog appears.
3. By default, the "Enable Ping Monitoring for this Server" checkbox is selected. If not, select it to enable the ping monitoring feature.
4. Provide the information required.

Field	Description
IP Address/Hostname	IP address or host name of the IT equipment whose accessibility you want to monitor.
Number of Successful Pings to Enable Feature	The number of successful pings required to enable this feature. Valid range is 0 to 200.
Wait Time (in seconds) after Successful Ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait Time (in seconds) after Unsuccessful Ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of Consecutive Unsuccessful Pings for Failure	The number of consecutive pings without any response before the IT equipment is declared unresponsive. Valid range is 1 to 100.
Wait Time (in seconds) before Resuming Pinging	The wait time before resuming pinging after the IT equipment is declared unresponsive. Valid range is 1 to 1200 (seconds).

5. Click OK to save the changes.

6. To add more IT devices, repeat Steps 2 to 5.
7. Click Close to quit the dialog.

Editing Ping Monitoring Settings

You can edit the ping monitoring settings for any IT device whenever it requires changes.

To modify the ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose settings you want to modify by clicking it.
3. Click Edit or double-click the IT device. The Edit Server 'XXX' dialog appears, where XXX is the IP address or host name of the IT device.
4. Make changes to the information shown.
5. Click OK to save the changes.

Deleting Ping Monitoring Settings

When it is not necessary to monitor the accessibility of any IT device, just remove it.

To delete ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose ping monitoring settings you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click Close to quit the dialog.

Environmental Sensors

Dominion PX can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed.

To add environmental sensors:

1. Physically connect environmental sensors to the Dominion PX device. See Connecting Environmental Sensors (Optional).

2. Log in to the Dominion PX web interface. Dominion PX should have detected the connected sensors, and display them in the web interface.
3. Identify each sensor through the sensor's serial number. See ***Identifying Environmental Sensors*** (on page 114).
4. Dominion PX should automatically manage the detected sensors. Verify whether detected sensors are managed. If not, have them managed. See ***Managing Environmental Sensors*** (on page 115).
5. Configure the sensors. See ***Configuring Environmental Sensors*** (on page 116). The steps include:
   a. Name the sensor.
   b. Mark the sensor's physical location in the rack or server room.

Identifying Environmental Sensors

A sensor includes a serial number tag on the sensor cable.

The serial number for each sensor appears listed with each sensor detected by Dominion PX in the web interface.

Match the serial number from the tag to those listed in the sensor table.

Managing Environmental Sensors

Dominion PX starts to retrieve an environmental sensor's reading and/or state and records the state transitions after the environmental sensor is managed.

The Dominion PX device can manage a maximum of 16 environmental sensors.

When there are less than 16 managed sensors, Dominion PX automatically brings detected environmental sensors under management. You should only have to manually manage a sensor when it is not under management.

To manually manage an environmental sensor:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Click the sensor you want to manage.

   Note: To identify all detected sensors, see **Identifying Environmental Sensors** *(on page 114).*

4. Click Manage. The "Manage sensor <serial number> (<sensor type>)" dialog appears, where <serial number> is the sensor's serial number and <sensor type> is the sensor's type.

   Note: For a contact closure sensor, a channel number is added to the end of the <sensor type>.

5. There are two ways to manage the sensor:
   - To manage this sensor and let Dominion PX assign a number to it, select "Automatically assign a sensor number." This method does not release any managed sensors.
   - To manage this sensor by assigning the number you want to it, select "Manually select a sensor number." Then click the drop-down arrow to select a number.

     If the number you assigned was occupied by a managed sensor, that sensor is released after losing its number.
6. Click OK. Dominion PX starts to track and display the sensor's reading and/or state.
7. To manage additional sensors, repeat Steps 3 to 6.

Note: When the number of managed sensors reaches the maximum, you CANNOT manage additional sensors until you remove or replace any managed sensors. To remove a sensor, see **Unmanaging Environmental Sensors** *(on page 122).*

Configuring Environmental Sensors

You may change the default name for easily identifying the managed sensor, and describe its location with X, Y and Z coordinates.

To configure environmental sensors:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Select the sensor that you want to configure.
4. Click Setup. The "Setup of external sensor <number>" dialog appears, where <number> is the number assigned to this sensor.
5. If the selected environmental sensor is the Raritan contact closure sensor connected with a third-party detector/switch, select the appropriate sensor type in the Binary Sensor Subtype field.
   - Contact: The detector/switch is designed to detect the door lock or door open/closed status.
   - Smoke Detection: The detector/switch is designed to detect the appearance of smoke.
   - Water Detection: The detector/switch is designed to detect the appearance of water on the floor.
   - Vibration: The detector/switch is designed to detect the vibration in the floor.
6. Type a new name in the Name field.
7. Describe the sensor's location by assigning alphanumeric values to the X, Y and Z coordinates. See ***Describing the Sensor Location*** (on page 118).
8. If the selected environmental sensor is a numeric sensor, its threshold settings are displayed in the dialog. Click Edit to adjust the threshold settings, including thresholds, deassertion hysteresis and assertion timeout.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.

- To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 100) for the function of deassertion hysteresis.
- To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. This value determines how many samples should be generated before any warning or critical condition is asserted. See ***What is Assertion Timeout?*** (on page 101).
- The Upper Critical and Lower Critical values are points at which Dominion PX considers the operating environment is critical and outside the range of the acceptable threshold.

9. Click OK to save the changes.

Setting the Z Coordinate Format

You can use either the number of rack units or a descriptive text to describe the vertical locations (Z coordinates) of environmental sensors.

To determine the Z coordinate format:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 53).*

2. Click Setup. The Pdu Setup dialog appears.
3. In the "External sensors Z coordinate" field, click the drop-down arrow and select an option from the list.
   - Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors.
   - Free-Form: Any alphanumeric string can be used for specifying the Z coordinate.
4. Click OK to save the changes.

Describing the Sensor Location

Use the X, Y and Z coordinates to describe each sensor's physical location. You can use these location values to track records of environmental conditions in fixed locations around your IT equipment. The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. If you choose to, you can use non-measurement values. For example:

X = *Brown Cabinet Row*

Y = *Third Rack*

Z = *Top of Cabinet*

Values for the X, Y and Z coordinates may consist of:

- For X and Y: Any combination of alphanumeric characters. The coordinate value can be 0 to 32 characters long.
- For Z when the Z coordinate format is set to *Rack Units*, any numeric value ranging from 0 to 60.
- For Z when the Z coordinate format is set to *Free-Form*, any alphanumeric characters from 0 to 32 characters.

Tip: To configure and retrieve these coordinate values over SNMP, see the Dominion PX MIB. To configure and retrieve these values over the CLI, see **Using the Command Line Interface** *(on page 142).*

Viewing Sensor Data

Readings of the environmental sensors will display in the web interface after these sensors are properly connected and managed.

The Dashboard page shows the information for managed environmental sensors only, while the External Sensors page shows the information for both of managed and unmanaged ones.

To view managed environmental sensors only:

1. Click the Dashboard icon in the Dominion PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the External Sensors section on the Dashboard page. The section shows:
   - Total number of managed sensors
   - Total number of unmanaged sensors
   - Information of each managed sensor, including:
     - Name
     - Reading

- State

To view both of managed and unmanaged environmental sensors:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.

   Detailed information for each connected sensor is displayed, including:

   - Label (number)
   - Serial number
   - Sensor type
   - Name
   - Reading
   - State
   - Channel (for a contact closure sensor only)

Sensor Measurement Accuracy

Raritan environmental sensors are with the following factory specifications. Calibration is not required for environmental sensors.

- Temperature: +/-2%
- Humidity: +/-5%

States of Managed Sensors

An environmental sensor shows the state after being managed.

Available sensor states vary depending on the sensor type -- numeric or discrete. For example, a contact closure sensor is a discrete sensor so it switches between three states only -- unavailable, alarmed and normal.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete sensors use alphabetical characters to indicate the state.

Sensor state	Applicable to
unavailable	All sensors
alarmed	Discrete sensors
normal	All sensors
below lower critical	Numeric sensors

Sensor state	Applicable to
below lower warning	Numeric sensors
above upper warning	Numeric sensors
above upper critical	Numeric sensors

"unavailable" State

The *unavailable* state means the connectivity to the sensor is lost.

Dominion PX pings all managed sensors at regular intervals in seconds. If it does not detect a particular sensor for three consecutive scans, the *unavailable* state is displayed for the sensor.

When the communication with a contact closure sensor's processor is lost, all detectors (that is, all switches) connected to the same sensor module show the "unavailable" state.

Note: When the sensor is deemed unavailable, the existing sensor configuration remains unchanged. For example, the ID number assigned to the sensor remains associated with it.

Dominion PX continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

"normal" State

This state indicates the sensor is in the normal state.

For a contact closure sensor, this state is the normal state you have set via the sensor's dip switch.

- If the normal state is set to Normally Closed, the *normal* state means the contact closure switch is closed.
- If the normal state is set to Normally Open, the *normal* state means the contact closure switch is open.

Note: See **Configuring a Contact Closure Sensor** *(on page 23) for setting the normal state.*

For a numeric sensor, this state means the sensor reading is within the acceptable range as indicated below:

Lower Warning threshold <= Reading < Upper Warning threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"alarmed" State

The state means the sensor is in the "abnormal" state, which is the opposite of the *normal* state. Only a discrete sensor shows this state.

For a contact closure sensor, the meaning of this state varies based on the sensor's normal state setting.

- If the normal state is set to Normally Closed, the *alarmed* state means the contact closure switch is open.
- If the normal state is set to Normally Open, the *alarmed* state means the contact closure switch is closed.

Tip: A contact closure sensor's LED is lit when in the alarmed *state. If the sensor module has two channels for connecting two switches, two LEDs are available. Check which contact closure switch is in the "abnormal" status according to the channel number of the LED.*

"below lower critical" State

Only a numeric sensor shows this state.

This state means the sensor reading is below the lower critical threshold as indicated below:

Reading < Lower Critical Threshold

"below lower warning" State

Only a numeric sensor shows this state.

This state means the sensor reading is below the lower warning threshold as indicated below:

Lower Critical Threshold <= Reading < Lower Warning Threshold

---

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper warningl" State

Only a numeric sensor shows this state.

This state means the sensor reading is above the upper warning threshold as indicated below:

Upper Warning Threshold <= Reading < Upper Critical Threshold

---

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper critical" State

Only a numeric sensor shows this state.

This state means the sensor reading is above the upper critical threshold as indicated below:

Upper Critical Threshold <= Reading

Note: The symbol <= means smaller than (<) or equal to (=).

Unmanaging Environmental Sensors

When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the Dominion PX device stops retrieving the sensor's reading and/or state.

To release a managed sensor:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 43).
2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Click the sensor you want to unmanage.
4. Click Release.

After a sensor is removed from management, the ID number assigned to the sensor is released and can be automatically assigned to any new sensor.

Asset Management

Configure the asset management settings only when an asset sensor is physically connected to the Dominion PX device.

Configuring the Asset Sensor

Dominion PX cannot detect how many rack units a connected asset sensor supports so you must provide this information manually.

To prevent the sensor LEDs from being lit permanently, enable LED scan mode so they are lit upon scan. This saves power.

To configure an asset sensor (Asset Strip):

1. Click the asset sensor in the left pane. The asset sensor's page opens in the right pane.

   Note: The asset sensor is named "Asset Strip 1" by default. The name changes after being customized.

2. Click Configure Asset Strip or double-click the asset sensor. The setup dialog for the selected asset sensor appears.

   Tip: You can also trigger the same dialog by clicking Asset Management in the left pane, selecting the asset sensor in the right pane, and clicking Configure Asset Strip.

3. To rename the asset sensor, type a new name in the Name field.
4. Type the total number of rack units the connected asset sensor supports in the Channel Count field. The web interface shows 48 rack units by default.
5. To enable LED scan mode, select the "enable" checkbox. **Optional**.
6. Click OK to save the changes.

Setting Asset Sensor LED Colors

Each LED on the asset sensor indicate the presence and absence of a connected asset tag by changing its color.

You can configure or change the color settings for all LEDs on an asset sensor by following the procedure below.

This feature is accessible only by users with administrative privileges.

To set a different LED color:

1. Choose Device Settings > Asset Management. The Configure Asset Management Settings dialog appears.
2. In the "Color with connected Tag" field, either click a color or type the hexadecimal RGB value of the desired color, which will be used to indicate the presence of a connected tag.
3. In the "Color without connected Tag" field, either click a color or type the hexadecimal RGB value of the desired color, which will be used to indicate the absence of a connected tag.
4. Click OK to save the changes.

Tip: To make a specific LED's colors different from other LEDs, see **Changing a Specific LED's Color Settings** *(on page 123).*

Changing a Specific LED's Color Settings

You can change the color settings of a specific LED on the asset sensor so that the LED behaves differently from other LEDs.

To change an LED's settings:

1. Click the asset sensor in the left pane. The asset sensor's page opens in the right pane.

   Note: The asset sensor is named "Asset Strip 1" by default. The name changes after being customized.

2. Select the rack unit whose LED settings you want to change.
3. Click Configure Rack Unit or double-click the selected rack unit. The setup dialog for the selected rack unit appears.

4. Select either Auto or Manual Override as this LED's color settings.
   - Auto (based on Tag): This is the default setting. With this option selected, the LED follows the global LED color settings. See ***Setting Asset Sensor LED Colors*** (on page 123).
   - Manual Override: This option differentiates this LED's behavior. After selecting this option, you must select an LED mode and/or color to have the LED permanently be in the selected mode and/or show the selected color.
     - LED Mode: Select On to have the LED stay lit permanently, Off to have it stay off, or Blinking to have it blink all the time.
     - LED Color: If you select On or Blinking in the LED Mode field, select a color to be shown by clicking that color.
5. Click OK to save the changes.

Displaying the Asset Sensor Information

The hardware and software information of the connected asset sensor is available through the web interface.

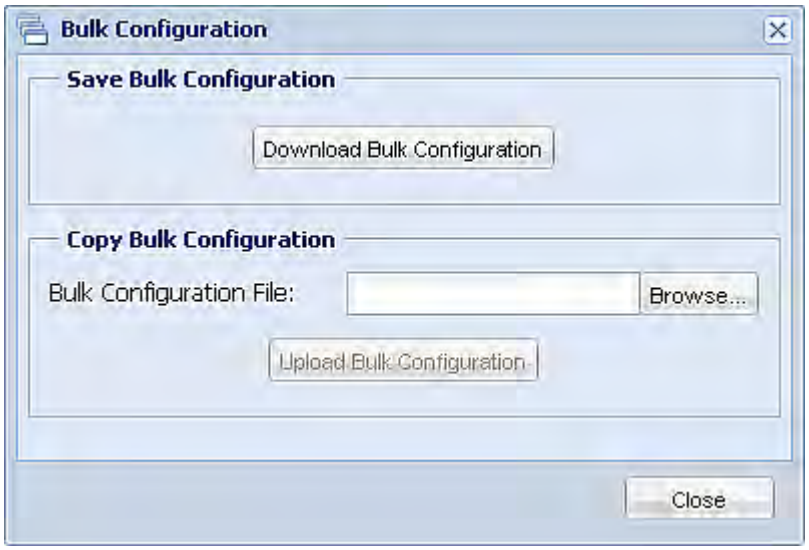
To display the asset sensor information:

1. Choose Maintenance > Device Information. The Device Information dialog appears.
2. Click the Asset Strips tab, where the asset sensor data is displayed.
3. Click Close to quit the dialog.

Copying Configurations with Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured Dominion PX device to your PC. This file can be used to copy that configuration to other Dominion PX devices of the same model or to restore the settings to previous configuration on the same Dominion PX device.

Users saving and copying Dominion PX configurations require the Administrator Privileges.



Saving a Dominion PX Configuration

A source device is an already configured Dominion PX device that is used to create a configuration file containing the settings that can be shared between Dominion PX devices. These settings include user and role configurations, thresholds, event rules, security settings, and so on.

This file does NOT contain device-specific information, including:

- Device name
- System name, system contact and system location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Outlet names
- Outlet status
- Environmental sensor names
- Environmental sensor states and values
- Certificate for SSL

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to Dominion PX devices in a different time zone than the source device.

To save a configuration file:

1. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
2. Click Download Bulk Configuration.
3. When the web browser prompts you to open or save the configuration file, click Save. Choose a suitable location and save the configuration file to your PC.

The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

Copying a Dominion PX Configuration

A target device is a Dominion PX device that loads another Dominion PX device's configuration file. Copying a Dominion PX configuration to a target device adjusts that Dominion PX device's settings to match those of the source Dominion PX device. In order to successfully restore a Dominion PX configuration:

- The user must be the Admin user. Or the Admin role is assigned to the user.
- The target Dominion PX device must be the same model type as the source Dominion PX device.
- The target Dominion PX device must be running the same firmware version as the source Dominion PX device.

To copy a Dominion PX Configuration:

1. Log in to the target device's web interface.
2. If the target device's firmware version does not match that of the source device, update the target's firmware. See ***Firmware Upgrade*** (on page 131).
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
4. In the Copy Bulk Configuration section, click Browse and select the configuration file on your PC.
5. Click Upload Bulk Configuration to copy the file. A message appears, prompting you to confirm the operation.
6. Click Yes to confirm the opeartion.
7. The Dominion PX device resets and the Login page re-appears, indicating that the configuration copy is complete.

Changing the Temperature Unit

Dominion PX can show temperatures in either Fahrenheit or Celsius based on the login name. The default temperature unit is Celsius. Only a user with the administrator privileges can change this setting for each user.

To set the preferred temperature unit:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. Click the Preferences tab.

5. In the Temperature Unit field, click the drop-down arrow, and select the desired option from the list.
   - °C: This option displays the temperature in Celsius.
   - °F: This option displays the temperature in Fahrenheit.
6. Click OK to save the changes.

Tip: You can determine the desired temperature unit when creating user profiles. See **Creating a User Profile** *(on page 64).*

Network Diagnostics

Dominion PX provides two tools on the web interface for troubleshooting potential networking issues.

- Ping
- Trace Route
- List TCP Connections

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 217).*

Pinging a Host

The Ping tool is useful for discovering whether a host is accessible through the network or Internet.

To ping a host:

1. Choose Maintenance > Network Diagnostics > Ping. The Ping Network Host dialog appears.
2. In the Host Name field, type the name or IP address of the host that you want to check.
3. In the Number of Requests field, type a number up to 10 or adjust the value by clicking either arrow. This number determines how many packets are sent for pinging the host.
4. Click Run Ping to start pinging the host. A dialog appears, displaying the Ping results.
5. Click Close to quit the dialog.

Tracing the Network Route

Trace Route lets you find out the route over the network between two hosts or systems.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > Trace Route. The Trace Route to Host dialog appears.
2. Type the IP address or name of the host whose route you want to check in the Host Name field.
3. Click Run. A dialog appears, displaying the Trace Route results.
4. Click Close to quit the dialog.

Listing TCP Connections

You can use the "List TCP Connections" to display a list of TCP connections.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > List TCP Connections. The TCP connections dialog appears.
2. Click Close to quit the dialog.

Viewing the Communication Log

Dominion PX allows you to inspect all communications occurred between the Dominion PX device and its graphical user interface (GUI). The information is usually useful for a technical support engineer only and you may not need to view it.

This feature is accessible only by users with administrative privileges.

To view the communication log:

1. Choose Maintenance > View Communication Log. The Communication Log dialog appears.
2. The dialog shows the last page by default. You can:
   - Switch between different pages by doing one of the following:

     - Click  or  to go to the first or last page.

     - Click  or  to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.
   - Select a log entry from the list and click Show Details to view detailed information of the selected entry.

Note: Sometimes when the dialog is too narrow, the icon » takes the place of the Show Details button. In that case, click » to view details.

3. To immediately update the communication log, click .
4. To save the communication log on your computer, click .
5. Enlarge the dialog if necessary. See ***Resizing a Dialog*** (on page 49).
6. You can re-sort the list or change the columns displayed. See ***Changing the View of a List*** (on page 48).
7. Click Close to quit the dialog.

Downloading Diagnostic Information

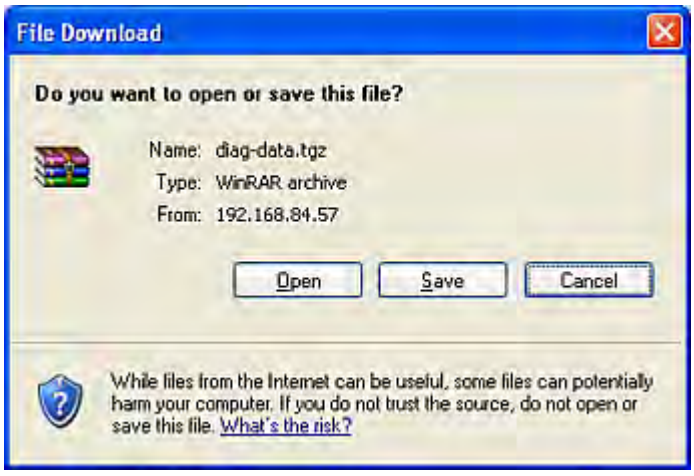
This function is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

You can download the diagnostic file from the Dominion PX device to a client machine. The file is compressed into a .tgz file and should be sent to Raritan Technical Support for interpretation.

This feature is accessible only by users with administrative privileges.

To retrieve a diagnostic file:

1. Choose Maintenance > Download Diagnostic Information. The File Download dialog appears.



2. Click Save. The Save As dialog appears.
3. Navigate to the desired directory and click Save.
4. E-mail this file as instructed by Raritan Technical Support.

Firmware Upgrade

You may upgrade your Dominion PX device to benefit from the latest enhancements, improvements and features.

Updating the Firmware

You must be the system administrator or log in to the user profile with the Firmware Update permission to update the Dominion PX device's firmware.

If applicable to your model, download the latest firmware file from the Raritan website, read the release notes, then start the upgrade. If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

Warning: Do NOT perform the firmware upgrade over a wireless connection.

To update the firmware:

1. Choose Maintenance > Update Firmware. The Firmware Update dialog appears.
2. In the Firmware File field, click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload status.
4. When the upload is complete, version information of both the existing firmware and uploaded firmware is shown, providing you a last chance to terminate the update.
5. To view the certificate of the uploaded firmware, click View Certificate. **Optional.**
6. To proceed with the update, click Update Firmware. The update may take several minutes.

   Warning: Do NOT power off the Dominion PX device during the update.

   During the firmware update:

   - A progress bar appears in the web interface, indicating the update status.
   - On the Dominion PX device, the three-digit LED display shows “FUP.”
   - No users can successfully log in to Dominion PX.
   - In the web interface, all logged-in users see the Dominion PX time out message, and the "disconnected" state is shown in the status bar.

- The user management operation, if any, is forced to suspend.

7. When the update is complete, a message appears, indicating the update is successful.
8. The Dominion PX device resets, and the Login page re-appears. You can now log in and resume your operation.

Note 1: The other logged-in users are also logged out when the firmware update is complete.

Note 2: If you are using Dominion PX with an SNMP manager, you should re-download the Dominion PX MIB after the firmware update. This ensures your SNMP manager has the correct MIB for the latest release you are using. See *Using SNMP* (on page 136).

A Note about Firmware Upgrade Time

The PDU firmware upgrade time varies from unit to unit, depending on various external and internal factors.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (which depends on the number of outlets). The microcontroller is upgraded only when required. Therefore, the length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated). Take the above factors into account when estimating the PDU's firmware upgrade time.

The time indicated in this note is for web-interface-based upgrades. Upgrades through other management systems, such as Raritan's Power IQ, may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

Viewing Firmware Update History

The firmware upgrade history, if available, is permanently stored on the Dominion PX device.

This history indicates when a firmware upgrade event occurred, the prior and new versions associated with the firmware upgrade event, and the upgrade result.

To view the firmware update history:

1. Choose Maintenance > View Firmware Update History. The Firmware Update History dialog appears, with the following information displayed.

- Date and time of the firmware upgrade event
- Previous firmware version
- Update firmware version
- Firmware upgrade result

2. You may change the number of displayed columns or re-sort the list for better viewing the data. See ***Changing the View of a List*** (on page 48).
3. To view the details of any firmware upgrade event, select it and click Details. The Firmware Update Details dialog appears, showing detailed information of the selected event.
4. Click Close to quit the dialog.

Full Disaster Recovery

If the firmware upgrade fails, causing the Dominion PX device to stop working, you can recover it by using a special utility rather than returning the PDU to Raritan.

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7 and Linux. In addition, an appropriate Dominion PX firmware file is required in the recovery procedure.

Updating the Asset Sensor Firmware

After connecting the asset sensor to the Dominion PX device, it automatically checks its firmware version against the version of the asset sensor firmware stored in the Dominion PX firmware. If the asset sensor firmware version on the Dominion PX device is different, the asset sensor automatically starts upgrading its firmware in the background.

During the firmware upgrade, the following events take place:

- The asset sensor is completely lit up, with the blinking LEDs changing the color from red to green.
- A firmware upgrade process is indicated in the Dominion PX web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.

Accessing the Help

The Help menu provides:

- Current firmware and software packages information
- A link to the Dominion PX User Guide (that is, the online help)

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the Dominion PX device through the web interface.

To retrieve the embedded software packages information:

1. Choose Help > About Dominion PX. The About Dominion PX dialog appears, with a list of open source packages displayed.
2. You can click any link in the dialog to access related information or download any software package.

Browsing through the Online Help

The Dominion PX User Guide is also provided in the form of online help, and accessible over the Internet.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriplets. Consult your browser help for information on enabling these features.

To use the Dominion PX online help:

1. Choose Help > User Guide. The online help opens in the default web browser.
2. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
3. To select a different topic, do any of the following:
   - To view the next topic, click the Next icon in the toolbar.
   - To view the previous topic, click the Previous icon.
   - To view the first topic, click the Home icon.
4. To expand or collapse a topic that contains sub-topics, do the following:
   - To expand any topic, click the white arrow prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow, and sub-topics appear below the topic.
   - To collapse any expanded topic, click the black, gradient arrow prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow, and all sub-topics below that topic disappear.
5. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon to start the search.

- If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

The search results are displayed in the left pane.

6. To have the left pane show the list of topics, click the Contents tab at the bottom.
7. To show the Index page, click the Index tab.
8. To email any URL link to the currently selected topic to any person, click the "Email this page" icon  in the toolbar.
9. To email your comments or suggestions regarding the user guide to Raritan, click the "Send feedback" icon  .
10. To print the currently selected topic, click the "Print this page" icon  .

Chapter 6 Using SNMP

This SNMP section helps you set up Dominion PX for use with an SNMP manager. Dominion PX can be configured to send traps to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

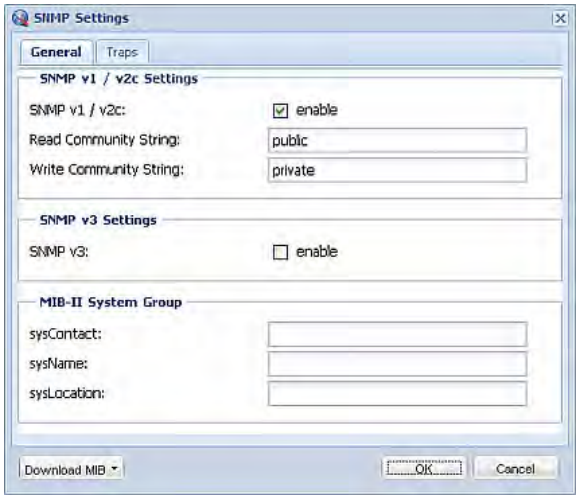
In This Chapter

Enabling SNMP

To communicate with an SNMP manager, you must first enable the SNMP agent on the Dominion PX device.

To enable SNMP:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.

- Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
- Type the read/write community string in the Write Community String field. Usually the string is "private."

3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

Tip: You can permit or disallow a user to access Dominion PX via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 137).*

4. Type the SNMP MIB-II sysContact value in the sysContact field.
5. Type the SNMP MIB-II sysName value in the sysName field.
6. Type the SNMP MIB-II sysLocation value in the sysLocation field.
7. Click OK to save the changes.

Important: You must download the SNMP MIB for your Dominion PX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see *Downloading SNMP MIB* (on page 139).

Configuring Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users need to have an Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between them and Dominion PX.

To configure users for SNMP v3 encrypted communication:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 64).
5. Click OK to save the changes. The user is now set up for encrypted SNMP v3 communication.

Configuring SNMP Traps

Dominion PX automatically keeps an internal log of events that occur. See ***Configuring Event Rules*** (on page 102). These events can also be used to send SNMP traps to a third party manager.

To configure Dominion PX to send SNMP traps:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the System SNMP Trap Rule.
3. Select the Enabled checkbox to enable this event rule.
4. Click Save to save the changes.
5. Click the Actions tab if you have not configured the SNMP trap actions.
6. Select System SNMP Trap Action to set up the trap destinations.
7. Type an IP address in the Host 1 field. This is the address to which traps are sent by the SNMP system agent.
8. Type the communication port number in the Port 1 field.
9. Type the name of the SNMP community in the Community field. The community is the group representing Dominion PX and all SNMP management stations.
10. To specify more than one SNMP trap destination, repeat Steps 8 to 10 for additional destinations. A maximum of 3 destinations can be specified.
11. Click Save to save the changes.
12. Click Close to quit the dialog.

Note: You should update the MIB used by your SNMP manager when updating to a new Dominion PX release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** *(on page 139).*

SNMP Gets and Sets

In addition to sending traps, Dominion PX is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about Dominion PX, such as the system location, and the current on a specific outlet.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the Dominion PX device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom Dominion PX MIB.

The Dominion PX MIB

The SNMP MIB file is required for using your Dominion PX device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Downloading SNMP MIB

The SNMP MIB file for Dominion PX can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

To download the file from the SNMP Settings dialog:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click Download MIB.
3. Click Save to save the file onto your computer.

Note: The above method downloads the PDU-MIB file.

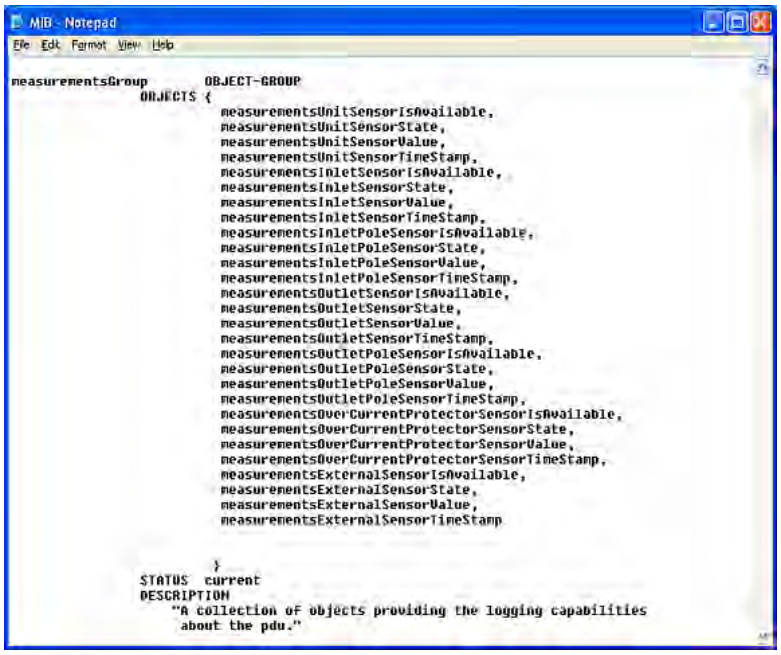
To download the file from the Device Information dialog:

1. Choose Maintenance > Device Information. The Device Information dialog appears.
2. Click the "download" link in the PDU-MIB or ASSETMANAGEMENT-MIB field to download the desired SNMP MIB file.
   - PDU-MIB: The SNMP MIB file for Dominion PX's power management.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for the Raritan asset management sensors.
3. Click Save to save the file onto your computer.

Layout

Opening the MIB reveals the custom objects that describe the Dominion PX system at the unit level as well as at the individual-outlet level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.



For example, the measurementsGroup group contains objects for sensor readings of Dominion PX as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the PDU current rating.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, causing Dominion PX to generate a warning and send an SNMP trap when certain parameters are exceeded. See ***Setting Power Thresholds*** (on page 98) for a description of how thresholds work.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure to set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 7 Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a Dominion PX device.

In This Chapter

About the Interface

Dominion PX provides a command line interface that enables data center administrators to perform some basic management tasks.

Using this interface, you can do the following:

- Reset the Dominion PX device
- Display the Dominion PX and network information, such as the device name, firmware version, IP address, and so on
- Configure the Dominion PX and network settings
- Troubleshoot network problems

You can access the interface over a serial connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Modifying the Network Service Settings** *(on page 57).*

Logging in to CLI

Logging in via HyperTerminal over a serial connection is a little different than logging in using SSH or Telnet.

With HyperTerminal

You can use any terminal emulation programs for local access to the command line interface.

This section illustrates HyperTerminal, which is part of Windows operating systems prior to Windows Vista.

To log in using HyperTerminal:

1. Connect your computer to the serial port on the Dominion PX device via a serial cable.
2. Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.

   Make sure serial port settings use this configuration:

   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None
3. Press Enter. The Username prompt appears.

   ```
   Username: _
   ```

4. Type a name and press Enter. The name is case sensitive, so make sure you capitalize the correct letters. Then you are prompted to enter a password.

   ```
   Username: admin
   Password: _
   ```

5. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters.

   After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 145) for details.

   Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to the Dominion PX web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the Dominion PX device.

With SSH or Telnet

You can remotely log in to the command line interface using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

To log in using SSH or Telnet:

1. Ensure SSH or Telnet has been enabled. See ***Modifying the Network Service Settings*** (on page 57).
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

```
login as:
```

3. Type a name and press Enter. The name is case sensitive, so make sure you capitalize the correct letters.

   Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

   Then you are prompted to enter a password.

```
login as: admin
admin@192.168.84.88's password:
```

4. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters.
5. After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 145) for details.

   Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to the Dominion PX web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the Dominion PX device.

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

- User Mode: When you log in as a normal user, who does not have full permissions to configure the Dominion PX device, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the Dominion PX device, the # prompt appears.
- Configuration Mode: You can enter the configuration mode from the administrator mode. In this mode, the prompt changes to **config:#** and you can change Dominion PX device and network configurations. See ***Entering the Configuration Mode*** (on page 158).
- Diagnostic Mode: You can enter the diagnostic mode from the administrator mode. In this mode, the prompt changes to **diag:>** and you can perform the network troubleshooting commands, such as the ping command. See ***Entering the Diagnostic Mode*** (on page 217).

Closing a Serial Connection

Close the window or terminal emulation program when you finish accessing a Dominion PX device over the serial connection.

When accessing or upgrading multiple Dominion PX devices, do not transfer the serial cable from one device to another without closing the serial connection window first.

Help Command

The help command shows a list of main CLI commands. This is helpful when you are not familiar with the commands.

▶ **The help command syntax is:**

```
#      help
```

Press Enter after typing the command, and a list of main commands is displayed.

Tip: You can check what parameters are available for a specific CLI command by adding a question mark to the end of the command. See **Querying Available Parameters for a Command** *(on page 215).*

Showing Information

You can use the show commands to view current settings or status of the Dominion PX device or part of it, such as the IP address, networking mode, firmware version, circuit breaker state, inlet ratings, and so on.

Many show commands have two formats: one with the parameter "details" and the other without. The difference is that the command without the parameter "details" displays a shortened version of information while the other displays in-depth information.

After typing a show command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt.

Network Configuration

This command shows the network configuration, such as the IP address, gateway, and subnet mask.

```
#       show network
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show network details
```

Wireless Configuration

This command shows the wireless configuration of the Dominion PX device, such as the SSID parameter.

```
#       show wireless
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show wireless details
```

PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version and model type.

```
#       show pdu
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show pdu details
```

Networking Mode

This command shows whether the current networking mode is wired or wireless. Currently Dominion PX supports the wired networking mode only.

```
#       show networkingMode
```

Network Service Settings

This command shows the network service settings, including the TCP ports for HTTP and HTTPS services.

```
#       show networkservices
```

Outlet Information

This command syntax shows the outlet information.

```
#        show outlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show outlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlets.
A specific outlet number	Displays the information for the specified outlet only.

Displayed information:

- Without the parameter "details," only the outlet name is displayed.
- With the parameter "details," more outlet information is displayed in addition to the outlet name, such as the outlet rating.

Inlet Information

This command syntax shows the inlet information.

```
#        show inlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show inlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all inlets.
A specific inlet number	Displays the information for the specified inlet only.

Displayed information:

- Without the parameter "details," only the inlet's L1, L2 and L3 current values and inlet name are displayed.
- With the parameter "details," more inlet information is displayed in addition to the RMS current values, such as the inlet's RMS current, voltage, and active power.

Inlet Pole Sensor Information

This command is available only for a three-phase PDU except for an inline monitor.

This command syntax shows the specified inlet pole sensor's information.

```
#       show sensor inletpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor inletpole <n> <p> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to query.
- <p> is the label of the inlet pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor

Sensor type	Description
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, hysteresis and assertion delay settings of the specified inlet pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy, resolution, tolerance, and range.
- If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

Circuit Breaker Information

This command is NOT available for a PDU without any overcurrent protection mechanism.

This command syntax shows the circuit breaker information.

```
#       show ocp <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show ocp <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all circuit breakers.
A specific circuit breaker number	Displays the information for the specified circuit breaker only.

Displayed information:

- Without the parameter "details," only the circuit breaker status and name are displayed.
- With the parameter "details," more circuit breaker information is displayed in addition to status, such as the rating and RMS current value.

External Sensor Information

This command syntax shows the environmental sensor's information.

```
#        show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show externalsensors <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all environmental sensors.
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensor page of the PDU's web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensory type and reading are displayed.

  Note: A discrete (on/off) sensor displays the sensor state instead of the reading.

- With the parameter "details," more environmental sensor information is displayed in addition to the ID and reading, such as the serial number and X, Y, and Z coordinates.

Circuit Breaker Sensor Information

This command is NOT available for a PDU without any overcurrent protection mechanism.

This command syntax shows the specified circuit breaker sensor's information.

```
#       show sensor ocp <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor ocp <n> <sensor type> details
```

Variables:

- <n> is the number of the circuit breaker whose sensors you want to query.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold and hysteresis settings of the specified circuit breaker sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy, resolution, tolerance, and range.
- If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

Environmental Sensor Information

This command syntax shows specified environmental sensor's information.

```
#       show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor externalsensor <n> details
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensor page of the PDU's web interface.

Displayed information:

- Without the parameter "details," only the reading, state, threshold, hysteresis and assertion delay settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy, resolution, tolerance, and range.
- If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

Note: For a discrete (on/off) sensor, only the sensor type and state are displayed no matter which command is performed.

Security Settings

This command shows the security settings of the Dominion PX device.

```
#       show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show security details
```

Displayed information:

- Without the parameter "details," the information including IP access control, role based access control, password policy, and HTTPS encryption is displayed.
- With the parameter "details," more sensor information is displayed, such as user blocking time and user idle timeout, is displayed.

Existing User Profiles

This command shows the data of one or all existing user profiles.

```
#       show user <user_name>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show user <user_name> details
```

Variables:

- <user_name> is the name of the user whose profile you want to query. The variable can be one of the options: *all* or a user's name.

Option	Description
all	This option shows all existing user profiles. *Tip: This is the default option. You can also leave out the "all" option to display all user profiles, that is, `show user`.*
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, "enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred temperature unit and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
#       show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. *Tip: This is the default option. You can also leave out the "all" option to display all roles, that is, `show roles`.*
a specific role's name	This option shows the data of the specified role only.

Displayed information:

- Role settings are displayed, including the role description and privileges.

Reliability Information

This command shows the reliability data.

```
#       show reliability data
```

This command shows the reliability error log.

```
#       show reliability errorlog
```

Command History

This command syntax shows the command history for current connection session.

```
#       show history
```

Displayed information:

- A list of commands that were previously entered in the current session is displayed.

History Buffer Length

This command syntax shows the length of the history buffer for storing the history commands.

```
#       show history bufferlength
```

Displayed information:

- The current history buffer length is displayed.

Examples

This section provides examples of the show command.

Example 1 - Basic Network Information

The diagram shows the output of the *show network* command.

```
# show network
Networking mode:       Wired
IP Configuration mode: DHCP

IP address:   192.168.84.58
Net mask:     255.255.255.0
Gateway:      192.168.84.254
#
```

Example 2 - In-Depth Network Information

More information is displayed when typing the *show network details* command.

```
# show network details
Networking mode:       Wired
IP Configuration mode: DHCP

IP address:   192.168.84.58
Net mask:     255.255.255.0
Gateway:      192.168.84.254
DNS servers:  192.168.80.19, 192.168.80.253
DNS suffixes: rgp.raritan.com
DHCP server:  192.168.80.4

Network interface speed:  Automatic
Network interface duplex: Automatic
Network interface state: Autonegotiation On, 100 Mbit/s, Full Duplex, Link OK

MAC address: 00:0d:5d:07:bb:30
#
```

Example 3 - Basic PDU Information

The diagram shows the output of the *show pdu* command.

```
# show pdu
PDU 'my PX'
Model:            PX2-5704U
Firmware version: 2.0.0.1.12880
#
```

Example 4 - In-Depth PDU Information

More information is displayed when typing the *show pdu details* command.

```
# show pdu details
PDU 'my PX'
Model:            PX2-5704U
Firmware version: 2.0.0.1.12880
Serial number:    PO79CE0199

Default outlet state on startup: Last known state
Power cycle delay:               10 seconds

Outlet power sequence:       default
Outlet power sequence delay: 200 ms

HTTP access port:  80
HTTPS access port: 443

Sensor data retrieval:      Disabled
Measurements per log entry: 60

Use Rack Units for sensor Z coordinate: Disabled
#
```

Configuring the Dominion PX Device and Network

To configure the Dominion PX device or network settings through the CLI, you must log in as the administrator.

Entering the Configuration Mode

You must enter the configuration mode since configuration commands function in the configuration mode only.

To enter the configuration mode:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `config` and press Enter. The config:# prompt appears, indicating that you have entered the configuration mode.

   ```
   config:# _
   ```

3. Now you can type any configuration command and press Enter to change the settings.

Important: To apply new configuration settings, you must issue the "apply" command before closing the terminal emulation program. Closing the program does not save any configuration changes. See *Quitting the Configuration Mode* (on page 215).

PDU Configuration Commands

A PDU configuration command begins with *pdu*. You can use the PDU configuration commands to change the settings that apply to the whole Dominion PX device.

The commands are case sensitive so ensure you capitalize them correctly.

Changing the PDU Name

This command syntax changes the Dominion PX device's name.

```
config:#   pdu name "<name>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "my px12" to the PDU.

```
config:#   pdu name "my px12"
```

Enabling or Disabling Data Logging

This command syntax enables or disables the data logging feature.

```
config:#   pdu dataRetrieval <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the data logging feature.
disable	Disables the data logging feature.

For more information, see ***Setting Data Logging*** (on page 62).

Example

The following command enables the data logging feature.

```
config:#   pdu dataRetrieval enable
```

Setting the Data Logging Measurements Per Entry

This command syntax defines the number of measurements accumulated per log entry.

```
config:#   pdu measurementsPerLogEntry <number>
```

Variables:

- <number> is an integer between 1 and 600. The default is 60 samples per log entry.

For more information, see ***Setting Data Logging*** (on page 62).

Example

The following command determines that 66 measurements are accumulated per log entry for internal sensors, that is, 66 seconds.

```
config:#   pdu measurementsPerLogEntry 66
```

Setting the Z Coordinate Format for Environmental Sensors

This command syntax enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:#   pdu externalSensorsZCoordinateFormat <option>
```

Variables:

- <option> is one of the options: *rackUnits* or *freeForm*.

Option	Description
rackUnits	The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors.
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

Note: After determining the format for the Z coordinate, you can set a value for it. See **Setting the Z Coordinate** *(on page 181).*

Example

The following command determines that the unit of rack is used for specifying the Z coordinate of environmental sensors.

```
config:#   pdu externalSensorsZCoordinateFormat rackUnits
```

Networking Configuration Commands

A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Setting the Networking Mode

If your Dominion PX device is implemented with both of the wired and wireless networking mechanisms, you must determine which mechanism is enabled for network connectivity before further configuring networking parameters.

This command syntax enables the wired or wireless networking mode.

```
config:#   networkingMode <mode>
```

Variables:

- <mode> is one of the modes: *wired* or *wireless*.

Mode	Description
wired	Enables the wired networking mode.
wireless	Enables the wireless networking mode.

Note: If you enable the wireless networking mode, and Dominion PX does not detect any wireless USB LAN adapter or the connected wireless USB LAN adapter is not supported, the message "Supported Wireless device not found" is displayed.

Example

The following command enables the wired networking mode.

```
config:#   networkingMode wired
```

Setting the Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *wireless*.

Note: If current networking mode is not wireless, the SSID, PSK and BSSID values are not applied until the networking mode is changed to "wireless." In addition, a message appears, indicating that the active network interface is not wireless.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the SSID

This command syntax specifies the SSID string.

```
config:#   wireless SSID <ssid>
```

Variables:

- <ssid> is the name of the wireless access point, which consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Example

The following command assigns "myssid" as the SSID.

```
config:#   wireless SSID myssid
```

Setting the PSK

This command syntax configures the PSK passphrase.

```
config:#   wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Example

This command assigns "encryp-key" as the PSK.

```
config:#   wireless PSK encryp-key
```

Setting the BSSID

This command syntax specifies the BSSID.

```
config:#   wireless BSSID <bssid>
```

Variables:

- <bssid> is the MAC address of the wireless access point.

Example

The following command specifies that the BSSID is 00:14:6C:7E:43:81.

```
config:#   wireless BSSID 00:14:6C:7E:43:81
```

Setting the Network Parameters

A network configuration command begins with *network*.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the IP Configuration Mode

This command syntax selects the IP configuration mode.

```
config:#   network ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IP configuration mode is set to DHCP.
static	The IP configuration mode is set to static IP address.

Example

The following command enables the Static IP configuration mode.

```
config:#   network ipConfigurationMode static
```

Changing the LAN Interface Speed

This command syntax determines the LAN interface speed.

```
config:#   network LANInterfaceSpeed <option>
```

Variables:

- <option> is one of the options: *auto*, *10Mbps*, *100Mbps* or *1000Mbps*. Note that the option "1000Mbps" is applicable only to the models implemented with the Gigabit Ethernet capability.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.
1000Mbps	The LAN speed is always 1 Gbps (for special models only).

Example

The following command lets Dominion PX determine the optimal LAN interface speed through auto-negotiation.

```
config:#   network LANInterfaceSpeed auto
```

Changing the LAN Duplex Mode

This command syntax determines the LAN interface duplex mode.

```
config:#   network LANInterfaceDuplexMode <mode>
```

Variables:

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	Dominion PX selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the Dominion PX device) at a time.

Option	Description
full	Full duplex: Data is transmitted in both directions simultaneously.

Example

The following command lets Dominion PX determine the optimal transmission mode through auto-negotiation.

```
config:#   network LANInterfaceDuplexMode auto
```

Setting the Preferred Host Name

After selecting DHCP as the IP configuration mode, you can specify the preferred host name, which is optional. The following is the command syntax:

```
config:#   network preferredHostName <name>
```

Variables:

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Example

The following command sets the preferred host name to "my-host."

```
config:#   network preferredHostName my-host
```

Setting the IP Address

After selecting the static IP configuration mode, you can use this command syntax to assign a permanent IP address to the Dominion PX device.

```
config:#   network ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your Dominion PX device. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command assigns the static IP address "192.168.84.222" to the Dominion PX device.

```
config:#   network ipAddress 192.168.84.222
```

Setting the Subnet Mask

After selecting the static IP configuration mode, you can use this command syntax to define the subnet mask.

```
config:#   network subnetMask <netmask>
```

Variables:

- <netmask> is the subnet mask address. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command sets the subnet mask to 192.168.84.0.

```
config:#   network subnetMask 192.168.84.0
```

Setting the Gateway

After selecting the static IP configuration mode, you can use this command syntax to specify the gateway.

```
config:#   network gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command sets the gateway to 255.255.255.0.

```
config:#   network gateway 255.255.255.0
```

Setting the Primary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the primary DNS server.

```
config:#   network primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command determines that the primary DNS server is 192.168.84.30.

```
config:#   network primaryDNSServer 192.168.84.30
```

Setting the Secondary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the secondary DNS server.

```
config:#   network secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command determines that the secondary DNS server is 192.168.84.33.

```
config:#   network secondaryDNSServer 192.168.84.33
```

Overriding the DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option disables the overriding and resumes using the DHCP-assigned DNS server.

Example

The following command overrides the DHCP-assigned DNS server with the one you specified.

```
config:#   network overrideDNS enable
```

Setting the Network Service Parameters

A network service command begins with *networkservices*.

Changing the HTTP Port

This command syntax changes the HTTP port.

```
config:#   networkservices httpPort <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.

Example

The following command sets the HTTP port to 81.

```
config:#   networkservices httpPort 81
```

Changing the HTTPS Port

This command syntax changes the HTTPS port.

```
config:#   networkservices httpsPort <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.

Example

The following command sets the HTTPS port to 333.

```
config:#   networkservices httpsPort 333
```

Security Configuration Commands

A security configuration command begins with *security*.

IP Access Control

You can modify, add or delete an IP access control rule through the command line interface. An IP access control configuration command begins with *security ipAccessControl*.

Modifying the IP Access Control Parameters

There are different commands for modifying different IP access control parameters.

- **To enable or disable the IP access control feature, use this command syntax:**

  ```
  config:#   security ipAccessControl enabled <option>
  ```

- **To determine the default policy, use this command syntax:**

  ```
  config:#   security ipAccessControl defaultPolicy <policy>
  ```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.

Option	Description
false	Disables the IP access control feature.

- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify both of IP access control parameters at a time. See **Multi-Command Syntax** *(on page 214).*

Example

The following command sets up two parameters of the IP access control feature.

```
config:#    security ipAccessControl enabled true defaultPolicy accept
```

Results:

- The IP access control feature is enabled.
- The default policy is set to "accept."

Adding an IP Access Control Rule

Depending on where you want to add a new IP access control rule in the list, the command syntax for adding a rule varies.

▶ **To add a new IP access control rule to the bottom of the list, use this command syntax:**

```
config:#    security ipAccessControl rule add <ip_mask> <option>
```

▶ **To add a new IP access control rule and insert it above or below a specific rule number, use this command syntax:**

```
config:#    security ipAccessControl rule add <ip_mask> <option> <insert> <rule_number>
```

-- OR --

```
config:#   security ipAccessControl rule add <insert> <rule_number> <ip_mask> <option>
```

Variables:

- <ip_mask> is the combination of the IP address and mask values. For example, *192.168.94.222/24*.
- <option> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from the specified IP address(es).
drop	Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
reject	Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule's number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule's number = the specified rule number + 1

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Example

The following command adds a new IP access control rule and specifies its location in the list.

```
config:#   security ipAccessControl rule add 192.168.84.123/24 accept insertAbove 5
```

Results:

- A new IP access control rule is added, allowing all packets from the IP addrress 192.168.84.123 to be accepted.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Deleting an IP Access Control Rule

This command removes a specific rule from the list.

```
config:#   security ipAccessControl rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Example

The following command removes the 5th rule from the IP access control list.

```
config:#   security ipAccessControl rule delete 5
```

HTTPS Access

This command determines whether the HTTPS access to the Dominion PX web interface is forced. If yes, all HTTP access attempts are automatically directed to HTTPS.

```
config:#   security enforceHttpsForWebAccess <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the HTTPS access to the web interface.
disable	Disables the HTTPS access to the web interface.

Example

The following command disables the HTTPS access feature.

```
config:#   security enforceHttpsForWebAccess disable
```

Login Limitation

The login limitation feature contains various parameters that you can modify with different commands.

- **To enable or disable the single login feature, use this command syntax:**

```
config:#   security loginLimits singleLogin <option1>
```

- **To enable or disable the password aging feature, use this command syntax:**

```
config:#   security loginLimits passwordAging <option2>
```

- **To determine the password aging time interval, use this command syntax:**

```
config:#   security loginLimits passwordAgingInterval <value1>
```

- **To determine the idle timeout value, use this command syntax:**

```
config:#   security loginLimits idleTimeout <value2>
```

Variables:

- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

- <option2> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the password aging feature.
disable	Disables the password aging feature.

- <value1> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.
- <value2> is a numeric value in minutes set for the idle timeout. The timeout ranges from 1 to 1440 minutes (24 hours).

Tip: You can combine multiple commands to modify the login limitation parameters at a time. See **Multi-Command Syntax** *(on page 214).*

Example

The following command sets up three parameters for the login limitation feature.

```
config:#   security loginLimits singleLogin disable passwordAging enable
           passwordAgingInterval 90
```

Results:

- The single login feature is disabled.
- The password aging feature is enabled.
- The password aging interval is set to 90 days.

User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

▶ **To determine the maximum number of failed logins before blocking a user, use this command syntax:**

```
config:#   security userBlocking maximumNumberOfFailedLogins <value1>
```

▶ **To determine how long a user's login is blocked, use this command syntax:**

```
config:#   security userBlocking blockTime <value2>
```

Variables:

- <value1> is an integer between 3 and 10, or *unlimited*, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.
- <value2> is a numeric value in minutes.

Tip: You can combine multiple commands to modify the user blocking parameters at a time. See **Multi-Command Syntax** *(on page 214).*

Example

The following command sets up two user blocking parameters.

```
config:#   security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Strong Passwords

There are various commands to modify strong password parameters. These commands begin with `security strongPasswords`.

- **To enable or disable the strong password feature, use this command syntax:**

  ```
  config:#   security strongPasswords enabled <option1>
  ```

- **To determine the minimum length of the password, use this command syntax:**

  ```
  config:#   security strongPasswords minimumLength <value1>
  ```

- **To determine the maximum length of the password, use this command syntax:**

  ```
  config:#   security strongPasswords maximumLength <value2>
  ```

- **To determine whether a strong password includes at least a lowercase character, use this command syntax:**

```
config:#   security strongPasswords enforceAtLeastOneLowerCaseCharacter <option2>
```

- **To determine whether a strong password includes at least a uppercase character, use this command syntax:**

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option3>
```

- **To determine whether a strong password includes at least a numeric character, use this command syntax:**

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option4>
```

- **To determine whether a strong password includes at least a special character, use this command syntax:**

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter <option5>
```

- **To determine the number of previous passwords that should not be repeated when forcing the password change, use this command syntax:**

```
config:#    security strongPasswords passwordHistoryDepth <value3>
```

Variables:

- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

- <value1> is an integer between 8 and 32.
- <value2> is an integer between 16 and 64.
- <option2> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

- <option3> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

- <option4> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.
disable	No numeric character is required.

- <option5> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

- <value3> is an integer between 1 and 12.

Tip: You can combine multiple commands to modify several strong password parameters at a time. See **Multi-Command Syntax** *(on page 214).*

Example

The following command sets up seven strong passwords parameters.

```
config:#    security strongPasswords enable enforceAtLeastOneLowerCaseCharacter enable
            enforceAtLeastOneUpperCaseCharacter disable
            enforceAtLeastOneNumericCharacter enable enforceAtLeastOneSpecialCharacter
            disable passwordHistoryDepth 7
```

Results:

- The strong password feature is enabled.
- A strong password is required.
- The password must have at least one lowercase character.
- The password does not require uppercase characters.
- The password must have at least one numeric character.
- The password does not require special characters.
- When changing the password, users are prevented from repeating any of the previous 7 passwords.

Outlet Configuration Commands

An outlet configuration command begins with *outlet*. Such command allows you to configure an individual outlet.

Changing the Outlet Name

This command syntax names an outlet.

```
config:#   outlet <n> name "<name>"
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Win XP" to outlet 8.

```
config:#   outlet 8 name "Win XP"
```

Inlet Configuration Commands

An inlet configuration command begins with *inlet*. You can configure an inlet by using the inlet configuration command.

Changing the Inlet Name

This command syntax names an inlet.

```
config:#   inlet <n> name "<name>"
```

Variables:

- <n> is the number of the inlet that you want to configure. The value is an integer between 1 and 50.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "AC source" to the inlet 1.

```
config:#   inlet 1 name "AC source"
```

Circuit Breaker Configuration Commands

A circuit breaker configuration command begins with *ocp.* The command configures an individual circuit breaker.

Changing the Circuit Breaker Name

This command syntax names a circuit breaker.

```
config:#   ocp <n> name "<name>"
```

Variables:

- <n> is the number of the circuit breaker that you want to configure. The value is an integer between 1 and 50.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The command assigns the name "Email servers CB" to the circuit breaker 3.

```
config:#   ocp 3 name "Email servers CB"
```

Environmental Sensor Configuration Commands

An environmental sensor configuration command begins with *externalsensor*. You can configure the name and location parameters for an individual environmental sensor.

Changing the Sensor Name

This command syntax names an environmental sensor.

```
config:#   externalsensor <n> name "<name>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Setting the X Coordinate

This command syntax specifies the X coordinate of an environmental sensor.

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command sets the value "The 2nd cabinet" to the X coordinate of the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 xlabel "The 2nd cabinet"
```

Setting the Y Coordinate

This command syntax specifies the Y coordinate of an environmental sensor.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command sets the value "The 4th row" to the Y coordinate of the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 ylabel "The 4th row"
```

Setting the Z Coordinate

This command syntax specifies the Z coordinate of an environmental sensor.

```
config:#   externalsensor <n> zlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Tip: You can specify the Z coordinate using the rack units. See **Setting the Z Coordinate Format for Environmental Sensors** *(on page 160).*

Example

The following command sets the value "The 5th rack" to the Z coordinate of the environmental sensor with the ID number 4 after the Z coordinate's format is set to *freeForm*.

```
config:#   externalsensor 4 zlabel "The 5th rack"
```

Changing the Sensor Description

This command syntax provides a description for a specific environmental sensor.

```
config:#   externalsensor <n> description "<description>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command gives the description "humidity detection" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 description "humidity detection"
```

Sensor Configuration Commands

A sensor configuration command begins with *sensor*. You can use the commands to configure the threshold and hysteresis values for any sensor associated with the following items:

- Inlets
- Inlet poles (for three-phase PDUs only)
- Circuit breakers
- Environmental sensors

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold is being enabled.

Commands for Inlet Sensors

A sensor configuration command for inlets begins with *sensor inlet*.

Setting the Inlet's Upper Critical Threshold

This command syntax configures the Upper Critical threshold of an inlet.

```
config:#   sensor inlet <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the number of the inlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Sensor type	Description
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified inlet sensor.
disable	Disables the upper critical threshold for the specified inlet sensor.
A numeric value	Sets a value for the upper critical threshold of the specified inlet sensor without enabling or disabling the threshold.

Example

The following command enables the Upper Critical threshold for the inlet 1 RMS current.

```
config:#   sensor inlet 1 current upperCritical enable
```

Setting the Inlet's Upper Warning Threshold

This command syntax configures the Upper Warning threshold of an inlet.

```
config:#   sensor inlet <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the number of the inlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Sensor type	Description
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified inlet sensor.
disable	Disables the upper warning threshold for the specified inlet sensor.
A numeric value	Sets a value for the upper warning threshold of the specified inlet sensor without enabling or disabling the threshold.

Example

The following command sets the Upper Warning threshold for the inlet 1 RMS current to 27A.

```
config:#   sensor inlet 1 current upperWarning 27
```

Setting the Inlet's Lower Critical Threshold

This command syntax configures the Lower Critical threshold of an inlet.

```
config:#   sensor inlet <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the number of the inlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Sensor type	Description
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified inlet sensor.
disable	Disables the lower critical threshold for the specified inlet sensor.
A numeric value	Sets a value for the lower critical threshold of the specified inlet sensor without enabling or disabling the threshold.

Example

The following command disables the Lower Critical threshold for the inlet 1 RMS current.

```
config:#   sensor inlet 1 current lowerCritical disable
```

Setting the Inlet's Lower Warning Threshold

This command syntax configures the Lower Warning threshold of an inlet.

```
config:#   sensor inlet <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the number of the inlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Sensor type	Description
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified inlet sensor.
disable	Disables the lower warning threshold for the specified inlet sensor.
A numeric value	Sets a value for the lower warning threshold of the specified inlet sensor without enabling or disabling the threshold.

Example

The following command sets the Lower Warning threshold for the inlet 1 RMS current to 20A.

```
config:#   sensor inlet 1 current lowerWarning 20
```

Setting the Inlet's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of an inlet.

```
config:#   sensor inlet <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the number of the inlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor

Sensor type	Description
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified inlet sensor. See ***What is Deassertion Hysteresis?*** (on page 100) for how the deassertion hysteresis works.

Example

The following command sets the deassertion hysteresis for the inlet 1 RMS current to 0.3A.

```
config:#   sensor inlet 1 current hysteresis 0.3
```

Commands for Inlet Pole Sensors

A sensor configuration command for inlet poles begins with *sensor inletpole*.

Setting the Upper Critical Threshold for an Inlet Pole

This command syntax configures the Upper Critical threshold of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Sensor type	Description
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified inlet pole sensor.
disable	Disables the upper critical threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the upper critical threshold of the specified inlet pole sensor without enabling or disabling the threshold.

Example

The following command disables the Upper Critical threshold for the pole 3 (L3-L1) voltage of the inlet 1.

```
config:#   sensor inletpole 1 L3 voltage upperCritical disable
```

Setting the Upper Warning Threshold for an Inlet Pole

This command syntax configures the Upper Warning threshold of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified inlet pole sensor.
disable	Disables the upper warning threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the upper warning threshold of the specified inlet pole sensor without enabling or disabling the threshold.

Example

The following command sets the Upper Warning threshold for the pole 2 (L2-L3) voltage of the inlet 1 to 180V.

```
config:#   sensor inletpole 1 L2 voltage upperWarning 180
```

Setting the Lower Critical Threshold for an Inlet Pole

This command syntax configures the Lower Critical threshold of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified inlet pole sensor.
disable	Disables the lower critical threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the lower critical threshold of the specified inlet pole sensor without enabling or disabling the threshold.

Example

The following command enables the Lower Critical threshold for the pole 2 (L2-L3) voltage of the inlet 1.

```
config:#   sensor inletpole 1 L2 voltage lowerCritical enable
```

Setting the Lower Warning Threshold for an Inlet Pole

This command syntax configures the Lower Warning threshold of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor

Sensor type	Description
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified inlet pole sensor.
disable	Disables the lower warning threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the lower warning threshold of the specified inlet pole sensor without enabling or disabling the threshold.

Example

The following command sets the Lower Warning threshold for the pole 3 (L3-L1) voltage of the inlet 1 to 190V.

```
config:#   sensor inletpole 1 L3 voltage lowerWarning 190
```

Setting the Inlet Pole's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> hysteresis <value>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2

Pole	Label <p>	Current sensor	Voltage sensor
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified inlet pole sensor. See ***What is Deassertion Hysteresis?*** (on page 100) for how the deassertion hysteresis works.

Example

The following command sets the deassertion hysteresis for the pole 2 (L2-L3) voltage of the inlet 1 to 0.5A.

```
config:#   sensor inletpole 1 L2 current hysteresis 0.5
```

Commands for Circuit Breaker Sensors

A sensor configuration command for circuit breakers begins with *sensor ocp*.

Setting the Upper Critical Threshold for a Circuit Breaker

This command syntax configures the Upper Critical threshold of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified circuit breaker sensor.
disable	Disables the upper critical threshold for the specified circuit breaker sensor.
A numeric value	Sets a value for the upper critical threshold of the specified circuit breaker sensor without enabling or disabling the threshold.

Example

The following command sets the Upper Critical threshold for the 3rd circuit breaker to 16A.

```
config:#   sensor ocp 3 current upperCritical 16
```

Setting the Upper Warning Threshold for a Circuit Breaker

This command syntax configures the Upper Warning threshold of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified circuit breaker sensor.
disable	Disables the upper warning threshold for the specified circuit breaker sensor.
A numeric value	Sets a value for the upper warning threshold of the specified circuit breaker sensor without enabling or disabling the threshold.

Example

The following command enables the Upper Warning threshold for the 3rd circuit breaker.

```
config:#   sensor ocp 3 current upperWarning enable
```

Setting the Lower Critical Threshold for a Circuit Breaker

This command syntax configures the Lower Critical threshold of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified circuit breaker sensor.
disable	Disables the lower critical threshold for the specified circuit breaker sensor.
A numeric value	Sets a value for the lower critical threshold of the specified circuit breaker sensor without enabling or disabling the threshold.

Example

The following command sets the Lower Critical threshold for the 3rd circuit breaker to 5A.

```
config:#   sensor ocp 3 current lowerCritical 5
```

Setting the Lower Warning Threshold for a Circuit Breaker

This command syntax configures the Lower Warning threshold of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified circuit breaker sensor.
disable	Disables the lower warning threshold for the specified circuit breaker sensor.
A numeric value	Sets a value for the lower warning threshold of the specified circuit breaker sensor without enabling or disabling the threshold.

Example

The following command enables the Lower Warning threshold for the 3rd circuit breaker.

```
config:#   sensor ocp 3 current lowerWarning enable
```

Setting the Circuit Breaker's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified circuit breaker sensor. See ***What is Deassertion Hysteresis?*** (on page 100) for how the deassertion hysteresis works.

Example

The following command sets the deassertion hysteresis for the RMS current of the 3rd circuit breaker to 1A.

```
config:#   sensor ocp 3 current hysteresis 1
```

Commands for Environmental Sensors

A sensor configuration command for environmental sensors begins with *sensor externalsensor*.

Setting the Sensor's Upper Critical Threshold

This command syntax configures the Upper Critical threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature* or *humidity*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified environmental sensor.
disable	Disables the upper critical threshold for the specified environmental sensor.
A numeric value	Sets a value for the upper critical threshold of the specified environmental sensor without enabling or disabling the threshold.

Example

The following command sets the Upper Critical threshold of the environmental "temperature" sensor with the ID number 2 to 40 degrees Celsius.

```
config:#   sensor externalsensor 2 temperature upperCritical 40
```

Setting the Sensor's Upper Warning Threshold

This command syntax configures the Upper Warning threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature* or *humidity*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified environmental sensor.
disable	Disables the upper warning threshold for the specified environmental sensor.
A numeric value	Sets a value for the upper warning threshold of the specified environmental sensor without enabling or disabling the threshold.

Example

The following command enables the Upper Warning threshold of the environmental "temperature" sensor with the ID number 4.

```
config:#   sensor externalsensor 4 temperature upperWarning enable
```

Setting the Sensor's Lower Critical Threshold

This command syntax configures the Lower Critical threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature* or *humidity*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified environmental sensor.
disable	Disables the lower critical threshold for the specified environmental sensor.
A numeric value	Sets a value for the lower critical threshold of the specified environmental sensor without enabling or disabling the threshold.

Example

The following command sets the Lower Critical threshold of the environmental "humidity" sensor with the ID number 1 to 15%.

```
config:#   sensor externalsensor 1 humidity lowerCritical 15
```

Setting the Sensor's Lower Warning Threshold

This command syntax configures the Lower Warning threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature* or *humidity*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified environmental sensor.
disable	Disables the lower warning threshold for the specified environmental sensor.
A numeric value	Sets a value for the lower warning threshold of the specified environmental sensor without enabling or disabling the threshold.

Example

The following command disables the Lower Warning threshold of the environmental "humidity" sensor with the ID number 3.

```
config:#   sensor externalsensor 3 humidity lowerWarning disable
```

Setting the Sensor's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature* or *humidity*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See ***What is Deassertion Hysteresis?*** (on page 100) for how the deassertion hysteresis works.

Example

The following command sets the deassertion hysteresis of the environmental "temperature" sensor with the ID number 4 to 2 degrees Celsius.

```
config:#   sensor externalsensor 4 temperature hysteresis 2
```

Setting the Sensor's Assertion Timeout

This command syntax configures the assertion timeout value of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> assertionTimeout
           <value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The number is assigned and shown on the Dominion PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature* or *humidity*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <value> is a numeric value (in samples) that is assigned to the assertion timeout for the specified environmental sensor. See ***What is Assertion Timeout?*** (on page 101).

Example

The following command sets the assertion timeout of the environmental "temperature" sensor with the ID number 4 to 3 samples.

```
config:#   sensor externalsensor 4 temperature assertionTimeout 3
```

User Configuration Commands

Most of user configuration commands begin with *user* except for the password change command.

Creating a User Profile

This command syntax creates a new user profile.

```
config:#   user create "<name>" <option> <roles>
```

After performing the user creation command, Dominion PX prompts you to assign a password to the newly-created user. Then:

1. Type the password and press Enter.
2. Re-type the same password for confirmation and press Enter.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the newly-created user profile.
disable	Disables the newly-created user profile.

- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Example

The following command creates a new user profile and sets up two parameters for the new user.

```
config:#   user create "May" enable admin
```

Results:

- A new user profile "May" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Modifying a User Profile

A user profile contains various parameters that you can modify.

To change a user's password, use this command syntax:

```
config:#   user modify "<name>" <password>
```

After performing the above command, Dominion PX prompts you to enter a new password. Then:

1. Type a new password and press Enter.
2. Re-type the new password for confirmation and press Enter.

- **To change a user's full name, use this command syntax:**

  ```
  config:#   user modify "<name>" fullname "<full_name>"
  ```

- **To change a user's telephone number, use this command syntax:**

  ```
  config:#   user modify "<name>" telephoneNumber "<phone_number>"
  ```

- **To change a user's email address, use this command syntax:**

  ```
  config:#   user modify "<name>" eMailAddress "<email_address>"
  ```

- **To enable or disable a user profile, use this command syntax:**

  ```
  config:#   user modify "<name>" enabled <option1>
  ```

- **This command syntax determines whether the password change is forced when a user logs in to the specified user profile next time:**

```
config:#   user modify "<name>" forcePasswordChangeOnNextLogin <option2>
```

- **To enable or disable the SNMP v3 access to Dominion PX for the specified user, use this command syntax:**

  ```
  config:#   user modify "<name>" snmpv3Access <option3>
  ```

- **To determine the security level, use this command syntax:**

  ```
  config:#   user modify "<name>" securityLevel <option4>
  ```

- **This command syntax determines whether the authentication passphrase is identical to the password:**

```
config:#    user modify "<name>" usePasswordAsAuthenticationPassPhrase <option5>
```

- **To determine the authentication passphrase, use this command syntax:**

```
config:#    user modify "<name>" authenticationPassPhrase "<authentication_passphrase>"
```

- **This command syntax determines whether the privacy passphrase is identical to the authentication passphrase:**

```
config:#    user modify "<name>" useAuthenticationPassPhraseAsPrivacyPassPhrase <option6>
```

- **To determine the privacy passphrase, use this command syntax:**

```
config:#   user modify "<name>" privacyPassPhrase "<privacy_passphrase>"
```

- **To determine the authentication protocol, use this command syntax:**

  ```
  config:#   user modify "<name>" authenticationProtocol <option7>
  ```

- **To determine the privacy protocol, use this command syntax:**

  ```
  config:#   user modify "<name>" privacyProtocol <option8>
  ```

- **To change the role(s) of the specified user, use this command syntax:**

  ```
  config:#   user modify "<name>" roles <roles>
  ```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <password> is the current password for the specified user profile.
- <full_name> is a string comprising up to 32 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.
- <phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes.
- <email_address> is the email address of the specified user. The <email_address> variable must be enclosed in quotes.
- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.

Option	Description
false	No password change is forced on the user's next login.

- <option3> is one of the options: *enabled* or *disabled*.

Option	Description
enabled	Enables the SNMP v3 access permission for the specified user.
disabled	Disables the SNMP v3 access permission for the specified user.

- <option4> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

- <option5> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

- <authentication_passphrase> is a string used as an authentication passphrase, comprising up to 32 ASCII printable characters. The authentication passphrase must be enclosed in quotes.
- <option6> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.
false	Privacy passphrase is different from the authentication passphrase.

- <privacy_passphrase> is a string used as a privacy passphrase, comprising up to 32 ASCII printable characters. The privacy passphrase must be enclosed in quotes.
- <option7> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

- <option8> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** *(on page 214).*

Example

The following command modifies three parameters for the user profile -- May:

```
config:#   user modify "May" fullname "May Turner" enabled true snmpv3Access enabled
```

Results:

- The full name is specified as May Turner.
- The user profile is enabled.
- The user's SNMP v3 access permission is enabled.

Deleting a User Profile

This command syntax deletes an existing user profile.

```
config:#   user delete "<name>"
```

Example

The following command deletes the user profile -- May.

```
config:#   user delete "May"
```

Changing Your Own Password

This command syntax changes your password. This command does not begin with *user*.

```
config:#    password
```

After performing this command, Dominion PX prompts you to first enter the existing password and then the new password.

Example

To change your password, follow this procedure:

1. Type the following command and press Enter.

   ```
   config:#    password
   ```

2. Type the existing password and press Enter when the following prompt appears.

   ```
   Existing Password:
   ```

3. Type the new password and press Enter when the following prompt appears.

   ```
   New Password:
   ```

4. Re-type the new password for confirmation and press Enter when the following prompt appears.

   ```
   Confirm New Password:
   ```

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command syntax creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
config:#    role create "<name>" <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, the privilege should be followed by a colon and the argument(s).

```
config:#   role create "<name>" <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role.
- <argument1>, <argument2> and the like are arguments set for a particular privilege.

Example

The following command creates a new role and assigns privileges to the role.

```
config:#   role create tester firmwareupdate;viewEventSettings
```

Results:

- A new role "tester" is created.
- Two privileges are assigned to the role: firmware update and view event settings.

Modifying a Role

You can modify diverse parameters of an existing role, including the privileges assigned to the role.

To modify a role's description, use this command syntax:

```
config:#   role modify "<name>" description <description>
```

To add privileges to a specific role, use this command syntax:

Multiple privileges should be separated with a semi-colon.

```
config:#   role modify "<name>" addPrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and then the argument(s) after the privilege.

```
config:#   role modify "<name>" addPrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

- **To remove specific privileges from a role, use this command syntax:**

  Multiple privileges should be separated with a semi-colon.

```
config:#   role modify "<name>" removePrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

  If a specific privilege contains any arguments, add a colon and then the argument(s) after the privilege.

```
config:#   role modify "<name>" removePrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove the privileges that you want to remove.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role.
- <argument1>, <argument2> and the like are arguments set for a particular privilege.

Example

The following command modifies the privileges of the role "tester."

```
config:#   role modify tester addPrivileges changeAuthentication removePrivileges
           firmwareupgrade
```

Results:

- The "change authentication" privilege is added to the role.
- The "firmware upgrade" privilege is removed from the role.

Deleting a Role

This command syntax deletes an existing role.

```
config:#   role delete "<name>"
```

Example

The following command deletes an existing role.

```
config:#   role delete tester
```

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command and perform all of them at a time.

A multi-command syntax looks like this:

```
<setting 1> <value 1> <setting 2> <value 2> <setting 3>
<value 3> ...
```

Example 1 - Combination of IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IP address, subnet mask and gateway for the network connectivity simultaneously.

```
config:#   network ipAddress 192.168.84.225 subnetMask 255.255.255.0
           gateway 192.168.84.0
```

Results:

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

Example 2 - Combination of Upper Critical and Upper Warning Settings

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 3rd circuit breaker.

```
config:#    sensor ocp 3 current upperCritical enable upperCritical 25
            upperWarning enable upperWarning 20
```

Results:

- The Upper Critical threshold of the 3rd circuit breaker's RMS current is enabled.
- The Upper Critical threshold of the 3rd circuit breaker's RMS current is set to 25A.
- The Upper Warning threshold of the 3rd circuit breaker's RMS current is enabled.
- The Upper Warning threshold of the 3rd circuit breaker's RMS current is set to 20A.

Querying Available Parameters for a Command

If you are not sure what commands are available for a particular type of CLI command, you can have the CLI show them by adding a space and then a question mark to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

To query available network configuration parameters, the syntax is:

```
config:#    network ?
```

To query available role configuration parameters, the syntax is:

```
config:#    role ?
```

Quitting the Configuration Mode

Both of "apply" and "cancel" commands let you quit the configuration mode. The difference is that "apply" saves all changes you made in the configuration mode while "cancel" aborts all changes.

To quit the configuration mode, use either command:

```
config:#    apply
```

-- OR --

```
config:#    cancel
```

The # prompt appears after pressing Enter, indicating that you have entered the administrator mode.

Unblocking a User

If any user is blocked from accessing Dominion PX, you can unblock them over a serial connection.

To unblock a user:

1. Log in to the CLI interface using any terminal program via a serial connection. See ***With HyperTerminal*** (on page 143).
2. When the Username prompt appears, type `unblock` and press Enter.

```
Username: unblock
```

3. When the "Username to unblock" prompt appears, type the login name of the user to be unblocked and press Enter.

```
Username to unblock:
```

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting Dominion PX

You can reset Dominion PX to factory defaults or simply restart it using the CLI commands.

Restarting the PDU

This command restarts the Dominion PX device. It is not a factory default reset.

To restart the Dominion PX device:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the Dominion PX device.

```
#     reset pdu unit
```

-- OR --

```
#     reset pdu unit /y
```

3. If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the Username prompt appears, indicating the reset is complete.

Resetting to Factory Defaults

This command restores all settings of the Dominion PX device to factory defaults.

To reset Dominion PX settings, use either command:

```
#     reset factorydefaults
```

-- OR --

```
#     reset factorydefaults /y
```

See ***Using the Command Line Interface*** (see "***Using the CLI Command***" on page 238) for more information.

Network Troubleshooting

Dominion PX provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

Entering the Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

To enter the diagnostic mode:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `diag` and press Enter. The diag> prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying the DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag>      nslookup <host>
```

Variables:

- <host> is the name or IP address of the host whose DNS information you want to query.

Example

The following command checks the DNS information regarding the host 192.168.84.222.

```
diag>       nslookup 192.168.84.222
```

Showing the Network Connections

This command syntax displays network connections and/or status of ports.

```
diag>       netstat <option>
```

Variables:

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Example

The following command displays the server connections to your Dominion PX device.

```
diag>       netstat connections
```

Testing the Network Connectivity

This command syntax sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good, or the host is not being connected to the network.

```
diag>       ping <host>
```

Variables:

- <host> is the host name or IP address whose networking connectivity you want to check.

Options:

- You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number.
size <number2>	Determines the packet size. <number2> is an integer number in bytes.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds.

The command looks like this syntax when it includes all options:

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

Example

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag>       ping count 5 192.168.84.222
```

Tracing the Route

This command syntax traces the network route between your Dominion PX device and a network host.

```
diag>       traceroute <host>
```

Variables:

- <host> is the name or IP address of the host you want to trace.

Example

The following command displays the existing network routing for the host 192.168.84.222.

```
diag>       traceroute 192.168.84.222
```

Quitting the Diagnostic Mode

▶ **To quit the diagnostic mode, use this command:**

```
diag>       exit
```

The # prompt appears after pressing Enter, indicating that you have entered the administrator mode.

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. For some *unique* CLI commands, such as the "reset" command, you can easily complete them by pressing the Tab or Ctrl+i instead of typing the whole command word by word.

▶ **To have a unique command completed automatically:**

1. Type initial letters or words of the command. For example, type the first word of the "`reset factorydefaults`" command, that is, `reset`.

2. Press Tab or Ctrl+i until the complete command appears. For example, although you typed only one word for the reset command, the rest of the command appears after pressing Tab or Ctrl+i.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

To log out of the CLI:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `exit` and press Enter.

Appendix A Specifications

In This Chapter

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for Dominion PX varies from 50 to 60 degrees Celsius, depending on the model and certification standard (CE or UL). If necessary, contact Raritan Technical Support for this information for your model.

Specification	Measure
Max Ambient Temperature	50~60 degrees Celsius

Serial RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DCD	Input	Data
2	RxD	Input	Receive data (data in)
3	TxD	Output	Transmit data
4	DTR	Output	Data terminal ready
5	GND	—	Signal ground
6	DSR	Input	Data set ready
7	RTS	Output	Request to send
8	CTS	Input	Clear to send
9	RI	Input	Ring indicator

Sensor RJ-12 Port Pinouts

RJ-12 Pin/signal definition			
Pin No.	Signal	Direction	Description

RJ-12 Pin/signal definition			
1	+12V	—	Power (500mA, fuse protected)
2	GND	—	Signal Ground
3	RS485 (Data +)	bi-directional	Data Line +
4	RS485 (Data -)	bi-directional	Data Line -
5	GND	—	Signal Ground
6	1-wire		Used for Feature Port

Appendix B Equipment Setup Worksheet

Dominion PX Series Model _____

Dominion PX Series Serial Number _____

OUTLET 1	OUTLET 2	OUTLET 3
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 4	**OUTLET 5**	**OUTLET 6**
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Types of adapters

_____

Types of cables

_____

Name of software program

_____

Appendix C MAC Address

A label is affixed to a Dominion PX device, near the LED display, showing both the serial number and MAC address of the PDU.

If necessary, you can find the PDU's IP address through the MAC address by using commonly-used network tools. Contact your LAN administrator for assistance.

Appendix D LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

a. Determine user accounts and groups intended for Dominion PX

b. Create user groups for Dominion PX on the AD server

c. Configure LDAP authentication on the Dominion PX device

d. Configure roles on the Dominion PX device

In This Chapter

Step A. Determine User Accounts and Groups

Determine the user accounts and groups that are authenticated for accessing Dominion PX. In this example, we will create two user groups with different permissions. Each group will consist of two user accounts available on the AD server.

User groups	User accounts (members)
PX_User	usera
	pxuser2
PX_Admin	userb
	pxuser

Group permissions:

- The PX_User group will have neither system permissions nor outlet permissions.
- The PX_Admin group will have full system and outlet permissions.

Step B. Configure User Groups on the AD Server

You must create the groups for Dominion PX on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups for Dominion PX are named *PX_Admin* and *PX_User*.
- User accounts *pxuser*, *pxuser2*, *usera* and *userb* already exist on the AD server.

To configure the user groups on the AD server:

1. On the AD server, create new groups -- *PX_Admin* and *PX_User*.

   Note: See the documentation or online help accompanying Microsoft AD for detailed instructions.

2. Add the *pxuser2* and *usera* accounts to the PX_User group.
3. Add the *pxuser* and *userb* accounts to the PX_Admin group.
4. Verify whether each group comprises correct users.

Step C. Configure LDAP Authentication on the Dominion PX Device

You must enable and set up LDAP authentication properly on the Dominion PX device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See ***Modifying the Network Settings*** (on page 54) and ***Role of a DNS Server*** (on page 55).
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over SSL.
- The AD server uses the default TCP port *389*.

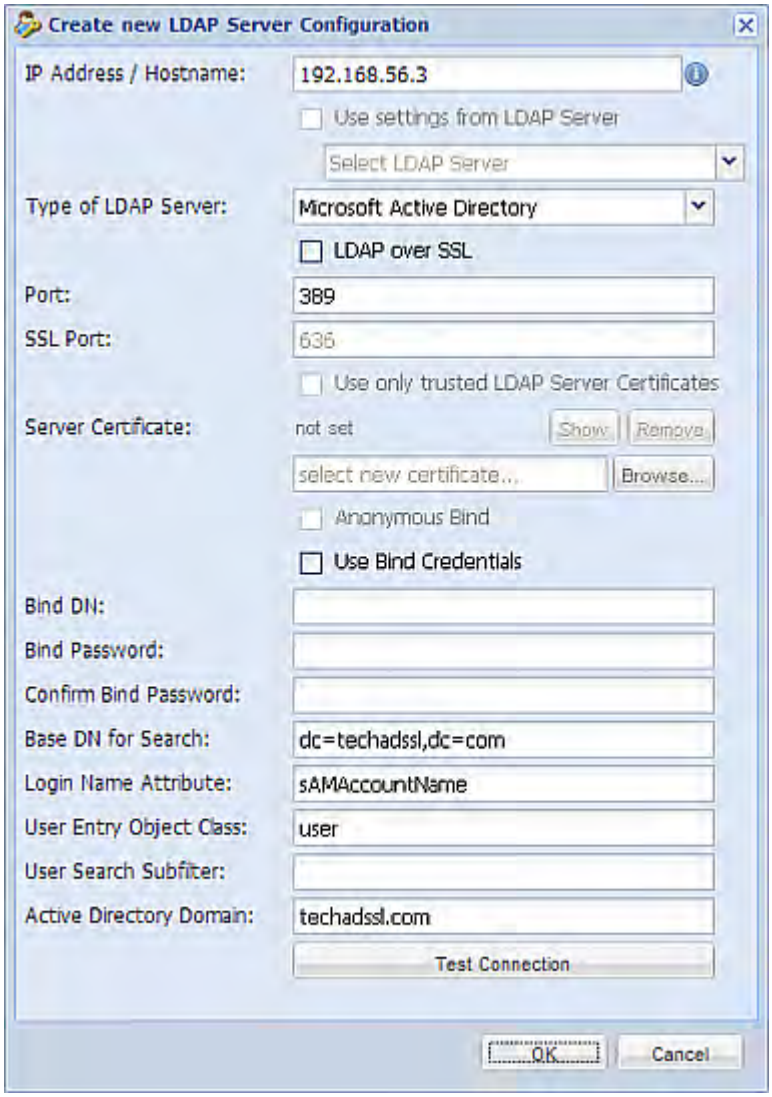
To configure LDAP authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate remote LDAP/LDAPS server authentication.
3. Click New to add an LDAP/LDAPS server for authentication. The "Create new LDAP Server Configuration" dialog appears.
4. Provide Dominion PX with the information about the AD server.
   - IP Address / Hostname - Type the domain name `techadssl.com` or IP address `192.168.56.3`.

   Important: Without the SSL encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the SSL encryption is enabled.

   - Use settings from LDAP server - Leave the checkbox deselected.
   - Type of LDAP Server - Select "Microsoft Active Directory" from the drop-down list.
   - LDAP over SSL - Have the checkbox deselected since the SSL encryption is not applied in this example.
   - Port - Ensure the field is set to `389`.
   - SSL Port and Server Certificate - Skip the two fields since the SSL encryption is not enabled.
   - Bind DN, Bind Password and Confirm Bind Password -- Skip the three fields since the selected type of LDAP server is Microsoft Active Directory.
   - Base DN for Search - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.

- Login Name Attribute - Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- User Entry Object Class - Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
- User Search Subfilter - The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
- Active Directory Domain - Type `techadssl.com`.



Note: For more information on LDAP configuration, see **Setting Up LDAP Authentication** *(on page 88).*

5. Click OK to save the changes. The LDAP server is saved.
6. Click OK to save the changes. The LDAP authentication is activated.

Note: If the Dominion PX clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure Dominion PX and the LDAP server to use the same NTP server.

Step D. Configure User Groups on the Dominion PX Device

A role on the Dominion PX device determines the system and outlet permissions. You must create the roles whose names are identical to the user groups created for Dominion PX on the AD server or authorization will fail. Therefore, we will create the roles named *PX_User* and *PX_Admin* on the PDU.

In this illustration, we assume:

- Users assigned to the *PX_User* role can neither configure Dominion PX nor access the outlets.
- Users assigned to the *PX_Admin* role have the Administrator permissions so they can both configure Dominion PX and access the outlets.

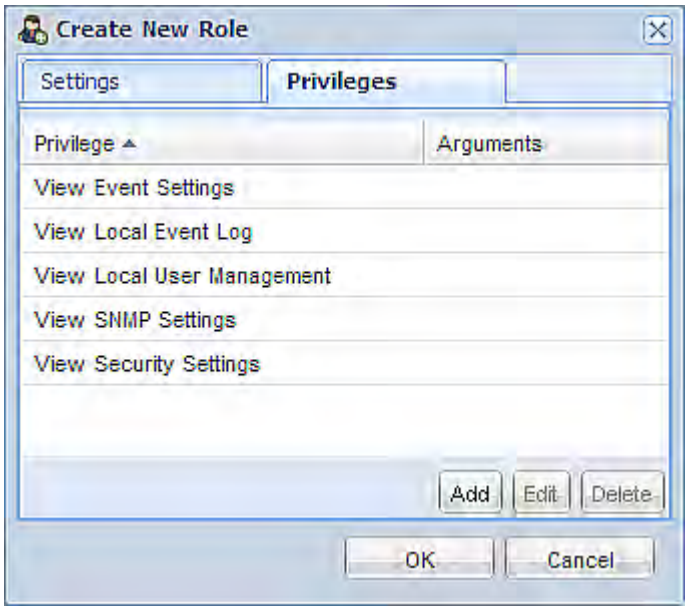
To create the PX_User role with appropriate permissions assigned:

1. Choose User Management > Roles. The Manage Roles dialog appears.

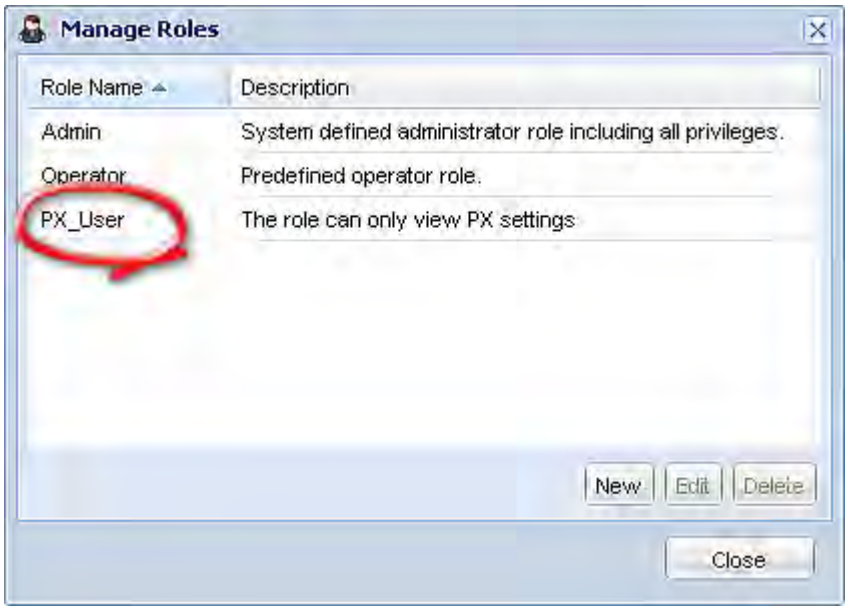
   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type `PX_User` in the Role Name field.
4. Type a description for the PX_User role in the Description field. In this example, we type "The role can only view PX settings" to describe the role.
5. Click the Privileges tab to select all View XXX permissions (where XXX is the name of the setting). A View XXX permission lets users view the XXX settings without the capability to configure or change them.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select a permission beginning with the word "View" from the Privileges list, such as View Event Settings.
   c. Click Add.

d. Repeat Steps a to c to add all permissions beginning with "View."



6. Click OK to save the changes. The PX_User role is created.

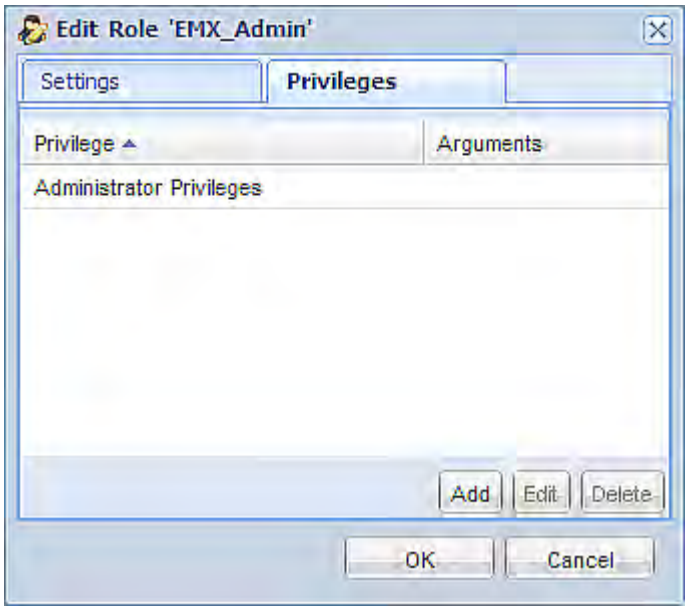


7. Keep the Manage Roles dialog opened to create the PX_Admin role.

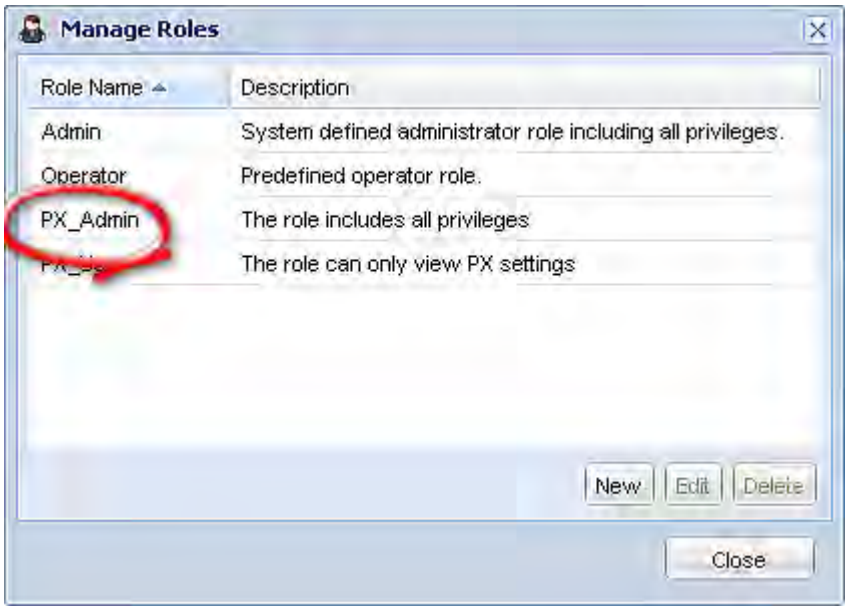
To create the PX_Admin role with full permissions assigned:

1. Click New. The Create New Role dialog appears.
2. Type `PX_Admin` in the Role Name field.

3. Type a description for the PX_Admin role in the Description field. In this example, we type "The role includes all privileges" to describe the role.
4. Click the Privileges tab to select the Administrator permission. The Administrator permission allows users to configure or change all Dominion PX settings.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission named Administrator Privileges from the Privileges list.
   c. Click Add.



5. Click OK to save the changes. The PX_Admin role is created.



6. Click Close to quit the dialog.

Appendix E Resetting to Factory Defaults

For security reasons, the Dominion PX device can be reset to factory defaults only at the local serial console.

Important: Exercise caution before resetting Dominion PX to its factory defaults. This erases any existing information and customized settings, such as user profiles and threshold values.

You can use either the reset button or the command line interface (CLI) to reset Dominion PX.

In This Chapter

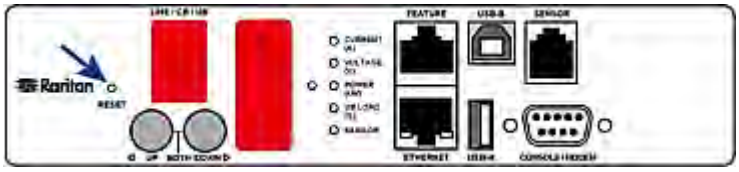
Using the Reset Button

This section describes how to reset the Dominion PX device via the reset button.

To reset to factory defaults using the reset button:

1. Connect a computer to the Dominion PX device over a serial connection.
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Dominion PX. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration*** (on page 16).
3. Press (and release) the Reset button of Dominion PX while pressing the Esc key of the keyboard several times in rapid succession. A prompt (=>) should appear after about one second.
4. Type *defaults* to reset the Dominion PX to its factory defaults.
5. Wait until the Username prompt appears, indicating the reset is complete.

The diagram shows the location of the reset button on Zero U models.



The diagram shows the location of the reset button on 1U models.

Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring Dominion PX to factory defaults. See ***Using the Command Line Interface*** (on page 142).

To reset to factory defaults using the CLI command:

1. Connect a computer to the Dominion PX device over a serial connection.
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Dominion PX. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration*** (on page 16).
3. Log in to the CLI by typing the user name "admin" and its password. See Step 4 of ***Initial Network Configuration*** (on page 16).
4. After the # system prompt appears, type either of the following commands and press Enter.

   ```
   #     reset factorydefaults
   ```

   -- OR --

   ```
   #     reset factorydefaults /y
   ```

5. If you entered the command without "/y" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.

6. Wait until the Username prompt appears, indicating the reset is complete.

Appendix F Non-Zero Readings While No Loads Attached

When no loads are physically attached to any outlets or lines, it is likely some Dominion PX models still show non-zero current or active power readings for the inlet in the web interface and/or LED display. This section explains why a PDU shows these readings when there are no loads attached.

- **The PDU shows non-zero current readings.**

  Reason: The current readings reflect the power consumption of the PDU's meter and controller boards. This is because the measurements are taken at the input lines to the PDU.

- **The PDU shows zero current readings while showing non-zero active power readings.**

  Reason: When no loads are connected, the PDU shows its own power consumption, usually a very low single-digit number, such as 2~3W. Power consumption varies depending on the rated voltage. For example, the active power reading shows 3W for 240V, but 6W for 120V. The PDU displays the current readings at the minimum of 1/10th of an ampere, such as 1.1A, 10.2A and the like. Without any loads attached, the current reading may show 0.0A because the current value is rounded off when the actual current value is below 1/10th of an ampere. For example, the actual current value for the 3W, 240V case is 0.0125A, which is shown as 0.0A after being rounded up to the 1/10th of an ampere.

Note: In this scenario, the active power reading for the inlet shows zero in the LED display, which is inconsistent with the corresponding reading shown in the web interface.

Index

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5991
Email: support.japan@raritan.com

Europe

Europe
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom
Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany
Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com